DATALAGRINGSDIREKTIVET – KRIMINALITETSBEKJEMPELSE PÅ BEKOSTNING AV PERSONVERNET?

Universitetet i Oslo

Det juridiske fakultet

Kandidatnummer: 549

Leveringsfrist: 26.04.10

Til sammen 17 796 ord

25.04.2010

Innholdsfortegnelse

1 Innledning

1.1 Om tema, problemstillingen og aktualitet

Personvernet i Norge har hatt en enorm utvikling siste halvdel av 1900-tallet.
Rt. 1952 s. 1217, om to mistenkelige personer, også kalt personverndommen, var den første høyesterettsavgjørelsen som slo fast at det fantes et ulovfestet personvern.[1] Et filmselskap ble under dissens (4-1) kjent uberettiget til å vise en film som bygget på en faktisk historie, av hensyn til det personlige rettsvern. Noen vil nok imidlertid si at det ulovfestede personvern kom til uttrykk allerede i Aarsdommen (Rt. 1896 s. 530) drøye 50 år tidligere.[2] Aarsdommen slo, på ulovfestet grunnlag, fast at en person har rett til beskyttelse av sitt spesielle slektsnavn. Avgjørelsen ble begrunnet utfra saksøkers personlige ønske om å beholde slektsnavnet Aars i sin egen familie.[3] Etter min mening synes Aarsdommen å være mindre relevant for denne oppgaven. Rt. 1991 s. 616, videoovervåkningskjennelsen, slo fast at videoopptak som arbeidsgiveren hadde foretatt i hemmelighet ikke kunne legges frem som bevis i en sak om underslag blant de ansatte. I kjennelsen ble det uttalt at hemmelig overvåking utgjør et alvorlig integritetsinngrep hos de ansatte og at det av hensyn til personvernet bør anses uakseptabelt. Avgjørelsen kom etter personregisterloven fra 1978, som var forløperen til dagens personopplysningslov fra 2000. Gjennom slutten av forrige århundre ble personvernet stadig styrket rettslig sett og gikk fra å være et ulovfestet vern til å bli lovfestet gjennom blant annet personopplysningsloven[4].

Etter terrorangrepene i New York 11. september 2001, Madrid 11. mars 2004 og i London 7. juli 2005 er man i økende grad blitt mer opptatt av høyere sikkerhet og kontroll i

[1] Bing (2002) s. 97

[2] Tokvam (1995) s. 15 og Schartum og Bygrave (2004) s. 252

[3] Tokvam (1995) s. 16

[4] Lov om behandling av personopplysninger av 14. april 2000 nr. 31

samfunnet. Dette er også bakgrunnen for EU-direktivet 2006/24/EF[5], populært kalt datalagringsdirektivet, som pålegger lagring av visse data med tanke på bekjempelse av grov kriminalitet, herunder terrorbekjempelse. Direktivet ble vedtatt av EU 15. mars 2006. EU-landene fikk frist til 15. september 2007 for å implementere det nasjonalt. Imidlertid med mulighet for å utsette gjennomføringen med tanke på kommunikasjonsdata fra Internett og e-post til 15. mars 2009. Det er fortsatt ikke avgjort hvorvidt direktivet skal implementeres i Norge. Dette skal opp til behandling i Stortinget i løpet av 2010.[6]

Jeg vil i denne oppgaven se nærmere på direktivet, både i forhold til gjeldende regelverk på området i Norge og forholdet til den europeiske menneskerettskonvensjon (EMK) art. 8. I dag er det i hovedsak lov om elektronisk kommunikasjon (ekomloven) og lov om behandling av personopplysninger (personopplysningsloven) som regulerer mulighetene for datalagring hos oss, med de begrensninger som måtte følge av EMK, jfr. menneskerettsloven § 3. Lov om rettergangen i straffesaker (straffeprosessloven) regulerer muligheten for utlevering av slike opplysninger til politiet. EMK art. 8 skal sikre enhver respekt for sitt privatliv og sin korrespondanse, herunder telefon, e-post og internettbruk.[7] Det har foreløpig ikke vært noen saker mot Norge om datalagring og forholdet til EMK art. 8 i den europeiske menneskerettsdomstol (EMD). Det er imidlertid uttrykt tvil om lagringsplikten som vil følge av en eventuell implementering av datalagringsdirektivet vil stride mot EMK art. 8.[8] Ettersom direktivet er såpass nytt har det enda ikke vært noen saker om det i EMD, men det finnes noe praksis som går på datalagring generelt i forhold til art. 8. I tillegg har direktivet vært oppe til rettslig vurdering i Romania og Tyskland. Det vil i denne oppgaven bli hovedfokus på nødvendighetskravet og kravet om forholdsmessighet.[9]

---

[5] Europa-parlamentets og rådets direktiv 2006/24/EF

[6] Datalagringsdirektivet er sendt på høring i januar 2010 med høringsfrist 12. april 2010

[7] Nordeide (2010) note 72

[8] NOU 2009:1 s. 190

[9] Jfr. EMK art. 8 annet ledd; ”*necessary in a democratic society”*

Problemstillingen er avgrenset til hvorvidt lagringsplikten etter datalagringsdirektivet, herunder lagringstid og hva som skal lagres, er i strid med retten til respekt for privatliv og korrespondanse i EMK art. 8. I kampen for et trygt samfunn utvikles det stadig sikkerhetsforanstaltninger og bestemmelser som skal motvirke kriminalitet. På den andre siden står blant annet hensynet til personvernet og den personlige integritet. Disse hensynene, som til dels kan være synes motstridende, må da veies opp mot hverandre ut fra proporsjonalitetsprinsippet. Proporsjonalitetsprinsippet er kommet til uttrykk gjennom EMK art. 8 annet ledd, og går i korthet ut på at inngrep i rettighetene beskyttet etter art 8 første ledd kun kan skje når det er forholdsmessighet mellom det en søker å oppnå med inngrepet og ulempene det medfører for de impliserte. Det kan spørres om hvor langt man er villig til å gå i kampen mot terror og grov kriminalitet, og om vi allerede har krysset den rettslige grensen for respekt for privatlivet. Vil en implementering av direktiv 2006/24/EF medføre ytterligere inngripen i et allerede presset personvern?

1.2 Avgrensning

Oppgaven er avgrenset til å behandle datalagringsdirektivets art. 5 og 6. Artiklene medfører at det som før var en lagringsadgang for teletilbydere nå blir en lagringsplikt dersom direktivet implementeres, samt en økt lagringstid i forhold til det lovverket i Norge hjemler i dag.

Når det gjelder vurderingen av direktivet opp mot personvernet er det bestemmelsen i EMK art. 8 jeg drøfter, og ikke forholdet til art. 17 i FN-konvensjonen om sivile og politiske rettigheter (SP), selv om innholdet i bestemmelsene er nesten likt. Avgrensningen er gjort av tidsmessige hensyn og det faktum at datalagringsdirektivet er et EU-direktiv og at forholdet til EMK således synes mest interessant og relevant å behandle.

Hva gjelder gjeldende regelverk, omfatter dette ekom- og personopplysningslovenes bestemmelser rundt teletilbyderes muligheter og forpliktelser for lagring av trafikkdata, konsesjonsvilkårene fra Datatilsynet og straffeprosesslovens regler om myndighetenes muligheter for å pålegge teletilbyderne å utlevere data.

Datalagringsdirektivet ble sendt ut på høring fra Samferdselsdepartementet i januar 2010 med høringsfrist 12. april. Det er såpass tett opp mot innleveringsdatoen for denne oppgaven at avhandlingen av tidsmessige grunner er avgrenset mot det som kommer frem i høringsrunden.

I min vurdering av direktivet har jeg valgt å ikke drøfte spørsmålet rundt økonomiske kostnader knyttet til implementeringen av direktivet, da det blir knapt med plass og jeg anser det som mindre relevant for min oppgave.

Det har i debatten rundt datalagringsdirektivet vært hevdet at rettstilstanden i Norge i dag strider mot EMK art. 8 og at direktivet må innføres for å oppfylle lovskravet i EMK art. 8.[10] Oppgaven min vil avgrense mot denne vurderingen rundt datalagringsdirektivet av plassmessige hensyn.

1.3 Begrepsforklaring

I det følgende vil jeg forklare en del tekniske begreper som vil gå igjen i oppgaven.

Data: Data er faktiske opplysninger, om for eksempel personer. Når enkeltdata blir trukket ut og satt sammen på en måte som gir mening for mottaker defineres det som informasjon.

Datalagring: Å lagre data til ulike formål for en viss tidsperiode, for eksempel til faktureringsformål.[11]

Elektronisk kommunikasjon: Elektronisk kommunikasjon er i ekomloven § 1-5 definert som all overføring av lyd, tekst, bilder eller annen data ved hjelp av elektromagnetiske signaler, enten det er i fritt rom eller i kabel i et signaltransportsystem.

---

[10] Bruce (2010) s. 13

[11] Teknologirådet (2007) *Oversikt over sikkerhetsteknologier* s. 61

Innholdsdata: Opplysninger om innholdet av en kommunikasjon, for eksempel hva noen snakket om i en telefonsamtale eller hvilke internettsider en har besøkt.

IP-adresse: En IP-adresse identifiserer en datamaskin. En nettserver vil lagre informasjon om hvilke(n) IP-adresse(r) som besøker hvilke nettsider.[12] Internettleverandører kan i dag lagre informasjon om hvilken kunde som har en bestemt IP-adresse i inntil tre uker.[13] IP-adresse kan også kalles elektronisk kommunikasjonsadresse.

Lokasjonsdata: Opplysninger som kan fortelle hvor et mobilt utstyr befant seg da det ble koblet opp, typisk ved bruk av mobiltelefon eller trådløs internettilgang.[14] Lokasjonsdata viser også hvor partene befant seg under en konkret samtale.

Personopplysning: En personopplysning er i personopplysningsloven definert som opplysninger og vurderinger som kan knyttes til en enkeltperson.[15] Disse opplysningene kan deles i to kategorier, "vanlige" personopplysninger og sensitive personopplysninger. Sensitive personopplysninger er opplysninger om rase, etnisk bakgrunn, politisk, filosofisk eller religiøs tilhørighet, helseforhold, seksuelle forhold, opplysninger om hvorvidt personen har vært utsatt for straffeforfølgning, samt medlemskap i fagforeninger.[16]

Personvern: Begrepet personvern er et norsk fenomen, i andre land brukes ofte betegnelser som "integrity" og "privacy". Man kan si at personvern er vern av ens personlige integritet[17] og individets ukrenkelighet. Denne definisjonen har også

[12] Teknologirådet (2007) *Oversikt oversikkerhetsteknologier* s. 23

[13] Brev fra Datatilsynet til IKT-Norge

[14] NOU 2009:1 s. 43

[15] Popplyl. § 2 nr. 1

[16] Popplyl. § 2 nr. 8

[17] NOU 1997:19 s. 17

personvernkommisjonen lagt til grunn. Innunder dette tolket kommisjonen ivaretakelse av enkeltindividets mulighet for privatliv, selvbestemmelse og selvutfoldelse.[18]

Personopplysningsvern: Personvernkommisjonen mener det må skilles mellom personvern og personopplysningsvern.[19] Kommisjonen definerer personopplysningsvern som regler og standarder for behandling av personopplysninger med personvern som et overordnet mål.[20] Denne oppfatningen bygger på Schartum og Bygrave sin bok som forklarer personopplysningsvern som en undergruppe av personvern som omfatter normer og regler for behandling av personopplysninger.[21]

Trafikkdata: Data som er nødvendig for å identifisere kilden og bestemmelsesstedet (sluttpunktet) for en kommunikasjon. Det vil si hvem som har ringt hvem når, men ikke innholdet av samtalen. I tillegg omfattes tidspunkt for inn- og utlogging (for internettbruk), start- og sluttidspunkt (for telefoni) og abonnementsidentifikasjon for telefoni og Internett, som for eksempel IP-adresser.[22]

1.4 Metode

Denne oppgaven er dels komparativ og dels rettspolitisk. Komparativ fordi oppgaven ser på forholdet mellom datalagringsdirektivet og EMK art. 8 og også forskjellen fra gjeldende rett rundt datalagring i Norge. Rettspolitisk fordi det i et tema som personvern også er naturlig å ta med noen rettspolitiske betraktninger.

Datalagringsdirektivet er såpass nytt at det foreligger svært lite rettspraksis rundt det. Det er imidlertid mange som har uttalt seg om direktivet, både av ulike organer, jurister og

[18] NOU 2009:1 s. 32

[19] NOU 2009:1 s. 32

[20] NOU 2009:1 s. 32

[21] Schartum og Bygrave (2004) s. 14

[22] NOU 2009:1 s. 43 og datalagringsdirektivet art. 2 a

professorer. Mye av kildematerialet er derfor juridisk litteratur, i tillegg til avgjørelser fra EMD om EMK art. 8.

Temaet personvern er et politisk tema så vel som juridisk og en del av kildematerialet vil naturlig nok være farget av det.

I forkant av Stortingets behandling av datalagringsdirektivet har blant annet Personvernkommisjonen og Datatilsynet kommet med uttalelser. Datatilsynet er et uavhengig forvaltningsorgan som ble opprettet for å påse at personopplysningsloven ble fulgt. Datatilsynet har både en ombuds- og tilsynsrolle.[23]

Personvernkommisjonen ble nedsatt i 2007 og skulle se på personvernet i møte med den teknologiske utviklingen.[24] Kommisjonens arbeid resulterte i rapporten *NOU 2009:1 Individ og integritet, personvern i det digitale samfunnet*. Kommisjonen bestod dels av personer med juridisk bakgrunn og dels av personer med annen faglig bagrunn, og hadde i utgangspunktet ikke et juridisk oppdrag og skulle ikke utarbeide konkrete lovforslag.[25] Personvernkommisjonen er nå avviklet.

Både Datatilsynet og Personvernkommisjonen har ivaretakelse av personvernet som formål. Uttalelser fra disse organene kan derfor bære preg av dette formålet. For å være sikret et nyansert bilde av datalagringsdirektivet er det derfor viktig å innhente informasjon fra andre organer i tillegg.

Ved vurderingen av hva som ligger i datalagringsdirektivet er det den engelske direktivteksten, samt høringsnotatet som Samferdselsdepartementet sendte ut i forbindelse med høringerunden for direktivet jeg har lagt til grunn. I notatet har

---

[23] Datatilsynet, *Om Datatilsynet*

[24] Pressemelding, Fornyings-, administrasjons- og kirkedepartementet

[25] NOU 2009:1 s. 13

Samferdselsdepartementet skissert opp noen forslag til hvordan direktivet kan tenkes implementert i Norge.

EMK finnes i to offisielle versjoner, på henholdsvis engelsk og fransk. Av språklige hensyn er det den engelske versjonen jeg har lagt til grunn ved tolkning av EMK art. 8.

I oktober 2009 falt det en dom i den rumenske forfatningsdomstolen om datalagringsdirektivet. Det finnes imidlertid ingen offisiell oversettelse av denne dommen. Jeg har derfor valgt å benytte meg av en engelsk oversettelse fra www.legi-internet.ro. Det må imidlertid tas i betraktning at det ikke er sikkert at denne oversettelsen er nøyaktig.
2. mars i år falt en dom i den tyske forfatningsdomstolen om implementeringen av datalagringsdirektivet i Tyskland. Jeg har ikke lyktes i å finne noen oversettelse av denne avgjørelsen, verken offisiell eller uoffisiell. I etterkant av domsavsigelsen i Tyskland kom det imidlertid en engelsk pressemelding fra den tyske forfatningsdomstolen, og det er denne jeg har benyttet for å redegjøre for resultatet av avgjørelsen.

2 Gjeldende rett i dag

I dag er det ekomloven, personopplysningsloven og datatilsynets konsesjonsvilkår som regulerer mulighetene for datalagring, og straffeprosessloven som regulerer mulig utlevering av lagrede data til politiet.

2.1 Ekomloven

Ekomloven (e-koml.) avløste den tidligere teleloven fra 1995. Ekomloven skal sikre brukerne gode og fremtidsrettede elektroniske kommunikasjonstjenester, jfr. e-koml. § 1-1. Loven gjelder for virksomhet knyttet til overføring av elektronisk kommunikasjon[26] samt tilhørende infrastruktur, tjenester, anlegg og utstyr, jfr. § 1-2. Det vil si at teletjenester, internettbasert kommunikasjon og generell internettbruk er omfattet av ekomloven.

I lovens andre kapittel er det intatt en rekke generelle bestemmelser rundt elektronisk kommunikasjon. Ekomloven § 2-7 hjemler en viss adgang til å lagre trafikkdata for teletilbydere. Trafikkdata utgjør blant annet opplysninger som er nødvendige for å fakturere en kunde for dennes bruk. Teletilbydere har mulighet til å lagre trafikkdata dersom det er nødvendig av faktureringsformål. Teletilbyderne er imidlertid forpliktet til å slette eller anonymisere trafikkdata straks de ikke lenger er nødvendig for kommunikasjons- eller faktureringsformål, jfr. e-koml. § 2-7 annet ledd. Etter forarbeidene[27] kan trafikkdata til bruk for faktureringsformål lagres frem til betaling har funnet sted eller til det er klart at fordringen ikke vil innfris. Øvrig behandling av trafikkdata, for eksempel til et annet formål, krever samtykke fra bruker i forkant av at behandlingen finner sted, jfr. e-koml. § 2-7 annet ledd annet punktum.

---

[26] Se forklaring av elektronisk kommunikasjon under punkt 1.3

[27] Ot.prp.nr. 58 (2002-2003) s. 72

Øvrig lokaliseringsdata må behandles i anonymisert form, med mindre brukeren har forhåndssamtykket og bruken av lokaliseringsdataene kun omfatter levering av en tilleggstjeneste som omfatter mer enn offentlig telefontjeneste. Også her skal behandlingen begrenses til et minimum, kun de data som er nødvendig for levering av tjenesten kan behandles.[28]

Ekomloven § 2-9 regulerer taushetsplikt. Den er en videreføring av bestemmelsen om taushetsplikt i den gamle teleloven fra 1995. Taushetsplikten innebærer at det teletilbydere får vite om andres bruk av elektronisk kommunikasjon, herunder trafikkdata, plikter de å bevare taushet om. De er også forpliktet til å forhindre at andre enn de(n) opplysningen(e) gjelder får tilgang til informasjonen. Rønnevig mener dette er en svakhet som ikke var tilsiktet videreført da teksten som er brukt må forstås som at teletilbyderen heller ikke kan benytte opplysningene i egen virksomhet til for eksempel faktureringsformål.[29] Dette har nok ikke vært meningen fra lovgivers side, noe som til dels kommer frem i forarbeidene.[30] Her sies det at hensikten var å videreføre den tidligere taushetspliktbestemmelsen i telegrafloven av 1899 § 5 hvor taushetsplikten gjaldt overfor "uvedkommende". Det at man tok ut ordet "uvedkommende" i teleloven av 1995 var ikke ment å medføre noen realitetsendring, og taushetsplikten i e-koml. § 2-9 første ledd må således tolkes innskrenkende. Ordet "bruk" er ment å omfatte tilbyders faktura samt data en får tilgang til på en mobiltelefon ved hjelp av PUK[31]-koden.[32]

Annet ledd utvider taushetsplikten til også å gjelde for de som får tilgang på opplysninger gjennom arbeid utført for teletilbyder, installatør, kontrollorgan eller myndighetene. Taushetsplikten vedvarer også etter at vedkommende som har fått tilgang på opplysningene har avsluttet oppdraget.

---

[28] Ekomforskriften § 7-2

[29] Rønnevig (2010) note 39

[30] Ot.prp. nr. 58 (2002-2003) s. 93

[31] Personal Unblocking Key, en personlig kode brukes for å låse opp en telefon når SIM-kortet er blitt sperret

[32] Rønnevig (2010) note 40a

Ekomloven § 2-9 tredje ledd åpner for en innskrenkning av taushetsplikten overfor påtalemyndigheten og politiet. Det gjelder opplysninger knyttet til teleabonnement, som blant annet avtalebasert hemmelig telefonnummer og elektronisk kommunikasjonsadresse, det vil si IP-adresse.[33] Opplysninger som kan kreves utlevert er navn og adresse tilhørende et hemmelig telefonnummer, samt navn, adresse og telefonnummer tilknyttet en IP-adresse. Etter Rt. 1999 s. 1944 ble det klart at "datakommunikasjonsadresse", som tilsvarer begrepet "elektronisk kommunikasjonsadresse" omfatter såkalte dynamiske IP-adresser.[34] Når en hadde nøyaktig tidspunkt for oppkoblingen som "entydig utpeker abonnenten" er det tilstrekkelig til at politiet kunne få utlevert navnet på abonnenten selv om dynamiske IP-adresser ikke er faste, men brukeren får tildelt et nytt nummer ved hver oppkobling.

Taushetsplikten i e-koml. § 2-9 forhindrer ikke at opplysninger gis til påtalemyndighet i medhold av annen lov, for eksempel straffeprosessloven, jfr. e-koml. § 2-9 tredje ledd siste punktum.

Ekomforskriften fra 2004 har ytterligere bestemmelser rundt kommunikasjonsvern. Ekomforskriften § 7-1 følger opp e-koml. § 2-7 og § 2-9 annet ledd om henholdsvis sletting og anonymisering og taushetsplikt. Forskriftens § 7-1 begrenser hvilke personer hos en teletilbyder som skal kunne behandle trafikkdata og hjemler et nødvendighetskriterium for denne behandlingen. Det er kun personer som jobber med fakturering, trafikkstyring, kundeforespørsler, markedsføring av elektroniske kommunikasjonstjenester eller med å avsløre ulovlig bruk av elektronisk kommunikasjon som har adgang til å behandle trafikkdata hos teletilbyderen, jfr. forskriftens § 7-1 annet ledd. Etter annet ledd siste punktum må behandlingen begrenses til det som er nødvendig for å utføre den konkrete arbeidsoppgaven. Dette forhindrer at en person som jobber med fakturering benytter seg av trafikkdata som kun er nødvendig i forhold til markedsføring av tjenester og omvendt.

---

[33] Se forklaring av IP-adresse under punkt 1.3

[34] Rønnevig (2010) note 42

2.2 Personopplysningsloven

Personopplysningsloven er ment å implementere EU-direktivet om behandling av personopplysninger og fri utveksling av slike opplysninger, direktiv 95/46/EF.

Datatilsynets konsesjonsvilkår for teletilbyders behandling av trafikkdata er hjemlet i personopplysningsloven.

Personopplysningsloven (popplyl.) har til formål å sikre den enkelte mot at personvernet blir krenket ved behandling av personopplysninger, jfr. popplyl. § 1. Loven skal sørge for at personopplysninger blir behandlet i tråd med de grunnleggende personvernhensyn. Med dette menes å sikre hensynet til den personlige integritet, respekt for privatlivets fred samt at personopplysninger skal ha tilstrekkelig kvalitet.

Loven er begrenset til behandling av personopplysninger som skjer med elektroniske hjelpemidler og annen behandling når personopplysningene skal inngå i et personregister hvor opplysningene er lagret systematisk slik at man enkelt kan finne opplysninger om en bestemt person igjen, jfr. popplyl. § 3 jfr. §2 nr. 3. Etter ordlyden i popplyl. § 3 omfattes ikke personopplysninger som en enkeltperson har samlet inn til personlig formål av loven. Personopplysningsloven § 3 gjennomfører art. 3 i direktiv 95/46/EF som blant annet sier at direktivet ikke får anvendelse på behandling av personopplysninger dersom det *"utføres av en fysisk person til rent personlige (...) aktiviteter"*. I Lindqvist-saken[35] ble rekkevidden av direktivets art. 3 drøftet. Saken gjaldt den svenske konfirmantlederen Bodil Lindqvist som hadde en hjemmeside på Internett. På denne siden hadde Lindqvist lagt ut opplysninger om 18 kollegers navn, delvis med fullt navn. Lindqvist omtalte også sine kollegers arbeidsoppgaver og deres fritidsinteresser. For flere av kollegaene var det lagt ut informasjon rundt familieforhold, samt telefonnumre, og for en av kollegaene var det lagt ut informasjon om at vedkommende var delvis sykemeldt som følge av et skadet ben. Domstolen slo fast at unntaket i art. 3 annet ledd ikke kom til anvendelse i Lindqvis- saken

[35] Sak C-101/01

da unntaket skal forstås som utelukkende for aktiveteter som inngår i den enkeltes privatliv, slik at opplysninger som en person legger ut på en nettside om andre enn seg selv og sin familie vil bli omfattet av reglene i personverndirektivet. Ettersom personopplysningsloven implementerer personverndirektivet i norsk rett må unntaket i popplyl. § 3 annet ledd forstås på samme måte.

Bestemmelsene i personopplysningsloven gjelder såfremt ikke annet følger av noen annen spesiallov om behandling av personopplysninger, som for eksempel helseregisterloven.[36]

For å behandle personopplysninger må enten personen opplysningene gjelder ha samtykket i en slik behandling, det må være fastsatt i lov eller det må være nødvendig etter et av vilkårene i popplyl. § 8 bokstav a til f.

Med samtykke fra personen menes en *"frivillig, uttrykkelig og informert erklæring"*[37] fra den det gjelder om at vedkommende godtar behandlingen. Det er ingen formkrav til erklæringen, men det må være klart at vedkommende har samtykket og hva han har samtykket i.[38] En passiv eller stilltiende aksept er ikke tilstrekkelig som en uttrykkelig erklæring, og et samtykke kan heller ikke skje i form av konkludent atferd.[39]

Nødvendighetsalternativet hjemler behandling av personopplysninger såfremt det er nødvendig for å ivareta visse interesser selv om det ikke foreligger samtykke fra vedkommende. Det er i forarbeidene[40] sagt at man i hovedsak bør basere behandlingen på samtykke og ikke på nødvendighet, ettersom vilkårene i bokstav a til f er relativt skjønnsmessige og det da kan oppstå tvil om hvorvidt de faktisk er oppfylt. Dette er fulgt

[36] Popplyl. § 5

[37] Popplyl. § 2 nr. 7

[38] Schartum (2010) note 14

[39] NOU 1997:19 s. 186

[40] Ot.prp.nr. 92 (1998-1999) s. 108

opp av Personvernnemda.[41] I PVN-2004-1 sa nemnda følgende om forholdet mellom samtykke og nødvendighet i popplyl. § 8:
"For at man skal kunne gjøre et avvik fra hovedprinsippet, må det derfor foreligge en begrunnelse. Denne begrunnelsen kan, som nevnt ovenfor, ikke bare være en ren hensiktsmessighetsbetraktning, f. eks. å unngå kostnader, spare tid eller lignende - selv om slike begrunnelser selvsagt også må vurderes konkret i forhold til den enkelte sak."

Et slikt avvik fra hovedprinsippet kan man finne i saker om arbeidsgivers kontrolltiltak, som for eksempel narkotikatesting av ansatte. Personvernemnda har i et slikt tilfelle uttalt at samtykke alene ikke er nok for å behandle personopplysninger etter popplyl. § 8.[42] Dette har nok sammenheng med det "avhengighetsforhold" en arbeidstaker kan føle til en arbeidsgiver.

Popplyl. § 11 oppstiller en del krav til den som behandler personopplysninger. Etter bokstav a er det et grunnkrav at opplysningene kun behandles når det er tillatt etter popplyl. § 8 og § 9. Dette virker ganske klart da samtlige tre er bestemmelser i lovens andre kapittel om alminnelige regler for behandling av personopplysninger.

Popplyl. § 11 bokstav b bestemmer at opplysninger kun kan behandles når formålet er uttrykkelig angitt og det samtidig er saklig begrunnet i virksomheten til den behandlingsansvarlige. For eksempel at teletilbydere lagrer visse trafikkdata for å kunne fakturere kunden for den konkrete bruken i etterkant. Saklighetskravet er ment å begrense behandling av personopplysninger som ikke har noen tilknytning til virksomheten, men bør ikke tolkes for strengt.[43]

Videre er det etter bokstav c ikke lov å benytte personopplysningene i etterkant til *"formål som er uforenlige med det opprinnelige formålet"*, med mindre den registrerte personen

[41] PVN-2007-7 og PVN-2004-1

[42] PVN-2005-6

[43] Schartum og Bygrave (2004) s. 137

samtykker i det. Dette for å forhindre at opplysninger innhentet til en type bruk benyttes til et helt annet formål og kanskje mot den registrertes vilje. Ordet "uforenlig" er et skjønnsmessig ord og hva som ligger i det må tolkes. Schartum mener det må bero på en konkret vurdering, men at dersom det nye formålet virker mot de opprinnelige interesser behandlingen skulle fremme så må det anses uforenlig.[44] Dersom det nye formålet er innenfor det den registrerte med rimelighet må regne med at opplysningene kan kunne brukes til vil det neppe kunne anses som "uforenlig" med det opprinnelige formålet.[45]

I bokstav d er det oppstilt vilkår om at opplysningene må være tilstrekkelige og relevante for formålet med behandlingen, også her er det tale om kumulative vilkår. Hensikten med dette kravet er å unngå at opplysningene blir mer omfattende enn det som er nødvendig, dette følger og av personverndirektivets art. 6 nr 1 bokstav c som popplyl. § 11 bokstav d er ment å implementere.

Endelig er det i bokstav e et krav om at opplysningene må være korrekte og oppdaterte og at de ikke må lagres lenger enn nødvendig ut fra formålet. Dette grunnkravet til behandling av personopplysninger stemmer overens med regelen i popplyl. § 28 som oppstiller et forbud mot lagring av unødvendige personopplysninger. Grunnkravene som er angitt i bokstav a til e er kumulative.

Personopplysningsloven § 11 annet ledd åpner for en senere behandling av personopplysninger dersom det er til historiske, statistiske eller vitenskapelige formål selv om det vil være uforenlig med det opprinnelige formålet. Bestemmelsen står dermed i sterk kontrast til grunnkravet i § 11 første ledd bokstav c. Slik behandling kan imidlertid kun skje dersom samfunnets interesse i at behandlingen skjer er klart større enn ulempene videre behandling har for den registrerte. Her må de to hensynene veies mot hverandre. Det må være en klar interesseovervekt for at videre behandling kan finne sted, jfr. ordlyden *"klart overstiger ulempene"* i § 11 annet ledd.

---

[44] Schartum (2010) note 53

[45] Schartum og Bygrave (2004) s. 137

Personopplysninger skal ikke lagres lenger enn det som er nødvendig ut fra formålet de er lagret for.[46] Dette gjelder uansett om opplysningene er lagret elektronisk eller i et manuelt personregister. Bestemmelsen skal sikre at behandling av personopplysninger avsluttes straks det ikke lenger er behov for lagring ut fra formålet, og at de ikke kan lagres på grunnlag av et annet formål enn det opprinnelige.[47] Denne bestemmelsen er bakgrunnen for at en internettleverandør ikke kan lagre informasjon om hvilken abonnent som er tildelt en IP-adresse lenger enn tre uker. Lagringen av informasjonen skjer for å ivareta driftsrelaterte formål og Datatilsynet konkluderte i 2009 med at dette formålet ikke ga grunnlag for en lengre lagringstid.[48]

Annet ledd i popplyl. § 28 gir muligheter for lagring av personopplysninger for historiske, statistiske eller vitenskapelige formål, men kun dersom samfunnets interesse i at opplysningene lagres er klart sterkere enn ulempene lagring medfører for den enkelte. Dersom opplysningene kan oppfylle formålet i anonymisert eller pseudonymisert form skal de anonymiseres eller pseudonymiseres så snart det er mulig.

Etter § 28 tredje ledd kan den registrerte kreve opplysningene om seg slettet dersom de er sterkt belastende for personen. Det skal imidlertid tungtveiende argumenter til for å få slettet opplysninger om seg selv hvis de er korrekte. Etter forarbeidene[49] skal vurderingen skje objektivt; det må oppfattes som svært belastende for folk flest. Endelig må slettingen være forsvarlig ut fra en totalvurdering av alle interesser.

For å behandle sensitive personopplysninger[50] kreves konsesjon fra Datatilsynet etter popplyl. § 33. Et unntak er for sensitive opplysninger som en person gir fra seg uoppfordret. Bestemmelsens andre ledd åpner for at Datatilsynet kan bestemme at det skal

---

[46] Popplyl. § 28 første ledd

[47] Ot.prp.nr. 92 (1998-1999) s. 125

[48] Datatilsynet, *Lagring av IP-adresse og abonnement - informasjon*

[49] Ot.prp.nr. 92 (1998-1999) s. 125

[50] Se forklaring av sensitive personopplysninger under punkt 1.3

være konsesjonsplikt også for personopplysninger som ikke er sensitive etter popplyl. § 2 nr. 8.

For at behandlingen av vanlige personopplysninger skal være konsesjonspliktige er det et krav at behandlingen av opplysningene åpenbart krenker tungtveiende personverninteresser. Ordlyden *"åpenbart krenker tungtveiende personverninteresser"* viser at vilkåret for at ikke-sensitive personopplysninger skal bli konsesjonspliktige er strengt. I forskriften til personopplysningsloven er det bestemmelser som gjør flere behandlinger av personopplysninger i blant annet telesektoren konsesjonspliktige, selv om det ikke er å regne som sensitive personopplysninger.

Personopplysningsforskriften § 7-1 fastslår at det er konsesjonsplikt for behandling av personopplysninger innenfor telesektoren. Konsesjonsplikten gjelder for teletilbyders behandling av personopplysninger i forbindelse med kundeadministrasjon, fakturering, og gjennomføring av tjenester forbundet til abonnentens bruk, jfr. forskriften § 7-1 første ledd. Teletilbydere er definert i andre ledd som virksomhet som i næringsøyemed tilbyr teletjenester ved hjelp av overføring i telenett, men kringkasting er ikke innbefattet. Etter popplyl. § 33 innvilges konsesjon av Datatilsynet og de har anledning til å sette nærmere vilkår for behandlingen i den grad det er nødvendig for å begrense skadevirkningene for den registrerte, jfr. popplyl. § 35.

2.2.1 Datatilsynets konsesjonsvilkår

Datatilsynet har utformet standard konsesjonsvilkår for teletilbydere som søker konsesjon etter popplyl. § 31 fjerde ledd for å behandle personopplysninger. Det er 11 vilkår som er gitt i medhold av popplyl. § 34 og § 35 som teletilbyder må følge gjennom hele konsesjonstiden.

Første vilkår fastsetter hva som skal være formålet med behandlingen. For teletilbydere er bruken av personopplysninger begrenset til det som er nødvendig i forbindelse med kundeadministrasjon, opplysningstjeneste, fakturering og gjennomføring av tjenester i

forbindelse med abonnentens bruk av telenettet. Behandling av personopplysninger til andre formål enn de som er listet opp i konsesjonsvilkårene punkt 1 kan kun skje i tråd med reglene i personopplysningsloven.

Selv om det ikke er angitt konkret hvilke opplysninger som kan behandles i konsesjonen er det begrenset til de opplysninger som er nødvendige for gjennomføring av tjenesten, jfr. vilkårene punkt 2. Dette er fullt forenlig med formålet i personopplysningsloven.

Punkt tre i vilkårene angir hvem som er behandlingsansvarlig for den konkrete konsesjonen og hvem som har det daglige ansvaret. Det påhviler den behandlingsansvarlige å sørge for at behandlingen er i samsvar med personopplysningsloven og dens forskrifter, samt at konsesjonen blir fulgt.

Etter konsesjonsvilkårene punkt 4 gjelder konsesjonen all behandling av personopplysninger som er knyttet til abonnentens bruk av telenett. Med abonnent menes enhver fysisk eller juridisk person som har inngått avtale om levering av offentlig tilgjengelige teletjenester med en leverandør.[51]

Opplysningene som skal behandles kan kun hentes inn fra abonnenten selv og gjennom hans bruk av teletjenestene i telenettet, jfr. konsesjonsvilkårene punkt 5. Med teletjeneste menes formidling av telekommunikasjon helt eller delvis ved overføring i telenett, men ikke kringkasting.[52] Definisjonen er således i samsvar med definisjonen av teletilbydere i personopplysningsforskriften §7-1, som er forklart ovenfor. Den behandlingsansvarlige skal sikre at de innsamlede opplysningene til enhver tid er korrekte, komplette og aktuelle for det formålet de er samlet inn for.

Etter punkt 6 skal personopplysningen ikke utleveres til utenforstående, med noen unntak. Opplysningene kan utleveres når den opplysningene omhandler har gitt samtykke til dette.

---

[51] Datatilsynet, *konsesjon teletjenester med merknader*

[52] Datatilsynet, *konsesjon teletjenester med merknader*

Samtykke skal her forstås som en frivillig, uttrykkelig og informert erklæring, noe som samsvarer med personopplysningslovens definisjon av begrepet, jfr. popplyl. § 2 nr. 7. Videre kan opplysninger utleveres med hjemmel i lov eller forskrift, for eksempel straffeprosessloven. Når det skjer skal den opplysningene gjelder informeres om utleveringen med mindre noe annet følger av lov. Opplysningene kan også utleveres dersom det er i forbindelse med betalingsinnkreving eller regnskapsbehandling. Det regnes ikke som utlevering at oppbevaringen eller behandlingen skjer hos et databehandlingsforetak dersom dette er på oppdrag fra den behandlingsansvarlige.

Uavhengig av punkt 6 åpner punkt 7 for utlevering av personopplysninger gjennom trykte eller elektroniske kataloger eller opplysningstjenester. Det er begrenset til opplysninger som er nødvendig for å identifisere en konkret abonnent, som navn, adresse og telefonnummer. Abonnenten må opplyses om oppføringen og reservasjonsmuligheten i katalog eller opplysningstjeneste i forkant av oppføringen og gis en rimelig frist til å reservere seg mot det. Dette innebærer et slags passivt samtykke. Dersom en vil ha med ytterligere opplysninger om kunden må disse derimot innhentes aktivt fra abonnenten.[53]

Punkt 8 i konsesjonsvilkårene regulerer sletting av de innsamlede opplysningene. Vilkårene er helt i samsvar med personopplysningsloven, hvilket innebærer at opplysninger som ikke har betydning for formålet skal slettes eller anonymiseres. Opplysninger som er brukt til faktureringsformål skal slettes når fakturaen er betalt. Det er en maksimumsfrist for lagring på tre måneder ved månedsvis fakturering og fem måneder ved kvartalsvis fakturering, så fremt det ikke oppstår tvist om kravet. I de tilfellene kan opplysningene lagres til tvisten er rettslig avgjort. Dette er i samsvar med bestemmelsen i e-koml. § 2-7.[54] Opplysninger som kun er nødvendig ved oppkobling eller gjennomføring av en teletjeneste skal slettes straks tilkoblingen er brutt. Dersom det er nødvendig å lagre opplysninger av hensyn til informasjonssikkerhet, gjøres det i henhold til personopplysningsforskriftens § 2-16 så

[53] Datatilsynet, *konsesjon teletjenester med meknader*

[54] Se punkt 2.1

lenge det er påkrevd. Kravet om sletting gjelder kun så langt det ikke er oppbevaringsplikt for opplysningene i medhold av annen lov.

Det er heller ikke tillatt å samkjøre opplysningene elektronisk slik at det dannes et nytt register. Videre er det ikke lov å sammenstille registeret med andre personregistre, med mindre det er hjemlet i lov. Et unntak er for sammenstilling av registre som eies av samme konsern. I slike tilfeller er det tillatt så langt det er nødvendig ut fra formålet med konsesjonen, jfr. konsesjonsvilkårene punkt 9.

Etter punkt 10 i konsesjonsvilkårene er teletilbydere forpliktet til å gi kundene uspesifisert faktura, med mindre noe annet er avtalt. En uspesifisert faktura vil si at verken telefonnumre, telekommunikasjonsadresser eller liknende fremkommer.

Endelig bestemmer konsesjonsvilkårene i punkt 11 at den behandlingsansvarlige hvert tredje år må sende Datatilsynet en bekreftelse på at behandlingen skjer i tråd med konsesjonssøknaden og personopplysningsloven.

2.3 Straffeprosessloven

Politiets adgang til lagrede trafikkdata er i dag regulert i straffeprosesslovens (strpl.) kapittel 16 og 16a. Hovedregelen om beslag og utlevering er strpl. § 203 som bestemmer at ting som er antatt å ha betydning som bevis kan beslaglegges inntil det foreligger en rettskraftig dom i den konkrete sak. Beslag besluttes av påtalemyndigheten dersom besitteren ikke vil utlevere tingen frivillig, jfr. strpl. § 205. Ved utlevering av trafikkdata fra teletilbyder kan også strpl. § 216b anvendes. Politiet kan ved kjennelse få tillatelse til å foreta kontroll av kommunikasjonsanlegg når en person med skjellig grunn mistenkes for en handling eller forsøk på dette som kan medføre fengselsstraff i minst fem år eller som rammes av straffeloven § 90, § 91, § 91a og § 94 (forbrytelser mot statens selvstendighet og sikkerhet), § 145 (datakriminalitet), § 162 og § 162c (narkotikakriminalitet), § 201a (pedofili), § 204a (pornografi), § 317 (heleri og hvitvasking) og § 390a (krenke annens person). Ved vilkåret om strafferamme på fem år er det den teoretiske strafferamme som er

avgjørende for vurderingen av om kravet om fem års fengselsstraff er oppfylt og ikke den forventede straff i en konkret sak.[55]

Etter § 216b annet ledd bokstav d kan denne kontrollen gå ut på å pålegge teletilbyder å gi politiet opplysninger om hvilke kommunikasjonsanlegg som i et konkret tidsrom har vært, eller skal settes i forbindelse med det kommunikasjonsanlegg den mistenkte har eller antas å ha benyttet. Slike opplysninger går under begrepet trafikkdata.

Straffeprosessloven § 215a ble innført 8. april 2005 for å gjennomføre Europarådets konvensjon av 8. november 2001 om bekjempelse av kriminalitet knyttet til informasjon og kommunikasjonsteknologi, jfr. lov av 8. april 2005. Den gir påtalemyndigheten mulighet til å pålegge sikring av elektronisk lagrede data som antas å ha betydning som bevis dersom det er som ledd i en etterforskning. Med elektronisk lagrede data siktes det her til både trafikkdata og innholdsdata.[56] Sikringspålegget kan ikke gis med virkning for fremtiden ettersom det er et krav om at dataene foreligger i elektronisk form når pålegget kommer.[57] Uttrykket *"antas å ha betydning"* vil si at det er tilstrekkelig med en rimelig mulighet, jfr. Rt. 1999 s. 2063. Videre er det i strpl. § 215a annet ledd et vilkår for å gi sikringspålegg til en teletilbyder at det er *"grunn til å tro at det er begått en straffbar handling"*. Uttrykket *"grunn til å tro"* skal forstås på samme måte som i § 222a.[58] Denne bestemmelsen ble tolket i Rt. 1998 s. 1638 og Høyesterett kom da til at det må være en nærliggende og reell risiko for at vedkommende har begått en straffbar handling, men det kreves ikke sannsynlighetsovervekt. Med andre ord kan ikke § 215a brukes til å gi pålegg om sikring av data for fremtiden, og heller ikke kan det gis basert på løse påstander om at en straffbar handling er begått. Det kreves at det er en viss sannsynlighet for at det er begått en kriminell handling før sikring av data iverksettes.

---

[55] Skaflem (2010) note 1509

[56] Se forklaring av begrepene under punkt 1.3

[57] Haugland (2010) note 1469

[58] Haugland (2010) note 1472

3 Innholdet i datalagringsdirektivet

Datalagringsdirektivet ble vedtatt med hjemmel i den daværende EF-traktaten artikkel 95, nå *traktaten om den europeiske unions funksjonsområde* (TEUF) art. 114.[59] Bestemmelsen hjemler tiltak for harmonisering av nasjonale lover og forskifter som angår det indre marked. Irland, med støtte fra Slovakia, reiste sak for EU-domstolen i 2006 for å få direktivet annullert fordi de mente det var vedtatt på feil grunnlag.[60] 10. februar 2009 tapte Irland saken. Domstolen kom til at det materielle innholdet av datalagringsdirektivet i hovedsak omhandler teletilbydernes virksomhet på det indre marked og ikke offentlige myndigheters kriminalitetsbekjempelse. Direktivet er derfor vedtatt på rett grunnlag. Dette medfører at direktivet trolig er EØS-relevant da direktiver vedtatt med hjemmel i TEUF art. 114[61] vanligvis er ansett å være innenfor det som omfattes av EØS-avtalen.[62]

3.1 Fra lagringsadgang til lagringsplikt

EU- og EØS-direktivet 2002/58/EF[63] (kommunikasjonsdirektivet) om databeskyttelse innenfor elektronisk kommunikasjon skulle sikre borgerne beskyttelse av privatlivets fred, også innenfor telesektoren. I Norge er dette direktivet i hovedsak implementert gjennom bestemmelser i ekomloven.[64] Lagrede trafikkdata skal etter art. 6 første ledd slettes eller anonymiseres straks de ikke lenger er nødvendig for gjennomføring av kommunikasjonen. Dette var ikke til hinder for at teletilbydere kunne lagre trafikkdata for en kort periode dersom det var nødvendig for faktureringsformål, jfr. direktivets art. 6 annet ledd. Etter

---

[59] EF-traktaten ble endret og fikk nytt navn etter at Lisboa-traktaten trådte i kraft i desember 2009

[60] Sak C-301/06 Irland mot Europa-parlamentet og Rådet for Den Europeiske Union

[61] Tidligere EFT art. 95

[62] Arnesen og Sejersted (2009) s. 3

[63] Europa-parlamentets og rådets direktiv 2002/58/EF av 12. juli 2002

[64] Schartum og Bygrave s. 104

art. 5 pålegges medlemsstatene å sikre borgerne kommunikasjonshemmelighet, ”*confidentiality of communications”,* ved bruk av det offentlige kommunikasjonsnett. Borgernes rett på hemmeligholdelse av sin kommunikasjon inkluderer også relaterte trafikkdata.[65] Lagring og mulig adgang til slike opplysninger kan etter art. 5 tredje ledd kun skje når abonnenten eller brukeren er klar over det, og den registrerte har rett til å nekte den registeransvarlige behandling av slike opplysninger. 25. november 2009 ble det vedtatt et direktiv[66] som blant annet gjør endringer i direktiv 02/58/EF. Direktiv 09/136/EC endrer art. 5 tredje ledd i direktiv 02/58/EF slik at lagring og adgang til de lagrede opplysninger ikke lenger kan nektes av abonnent eller bruker.[67] Direktiv 09/136/EC skal implementeres innen 25. mai 2011, jfr. art. 4. Da det endrer et EØS-relevant direktiv antar jeg at direktiv 09/136/EC også vil være EØS-relevant. Kommunikasjonsdirektivets art. 15 første ledd åpner for at medlemslandene gjennom nasjonal lovgivning kan innskrenke rekkevidden av visse bestemmelser i personverndirektivet[68] dersom det er *”nødvendig, passende og forholdsmessig i et demokratisk samfunn”.*[69] Datalagingsdirektivet art. 11 gjør en endring i kommunikasjonsdirektivets art. 15. Endringen går ut på at kommunikasjonsdirektivet art. 15 første ledd ikke gjelder for data som er lagret i medhold av datalagringsdirektivet.

Mens teletilbydere i medlemslandene tidligere hadde en adgang til å lagre trafikkdata medfører en implementering av datalagringsdirektivet en lagringsplikt for teletilbyderne. I den videre redegjørelsen for innholdet i datalagringsdirektivet legger jeg de engelske og danske versjonene til grunn, da det enda ikke er kommet en norsk versjon av direktivet.

Formålet med datalagringsdirektivet er å lagre visse kommunikasjonsdata, og sikre tilgang til de lagrede opplysningene for å etterforske, oppklare og straffeforfølge alvorlig kriminalitet, jfr. direktivets art. 1. I den offisielle engelske versjonen er uttrykket *”serious*

---

[65] Direktiv 02/58/EF art. 5 første ledd

[66] Europaparlementets og rådets direktiv 09/136/EC

[67] Direktiv 09/136/EC art. 2

[68] Direktiv 95/46/EF

[69] Direktiv 02/58/EF art. 15 første ledd

crime" benyttet, og det skal være opp til den enkelte stat å definere hva som i nasjonal rett vil være å anse som *"serious crime".* Direktivet har blitt kritisert fordi uttrykket *"serious crime"* er for vagt og ikke nærmere konkretisert.[70] Article 29 Working Party[71] (art. 29 WP) har i to uttalelser[72] kommet med sterk kritikk mot den vage formuleringen og anbefalt at formålet med lagringen blir klart definert og avgrenset til bekjempelse av terrorisme og organisert kriminalitet.[73] Disse uttalelsene ble det imidlertid ikke tatt hensyn til ved utformingen av den endelige direktivtekst, jfr. ordlyden i direktivets art. 1.

Artikkel 3 i datalagringsdirektivet pålegger medlemsstatene å lagre trafikk-, lokasjons- og brukerdata knyttet til telefoni og internettbruk.[74] Etter datalagringsdirektivet art. 3 første ledd får tilbydere av offentlig tilgjengelige elektroniske kommunikasjonstjenester, og av offentlige kommunikasjonsnett, en forpliktelse til å lagre visse data i overenstemmelse med direktivet. Hvilke konkrete data som skal lagres angis i direktivets art. 5.

3.2 Hva skal lagres?

Artikkel 5 inneholder en omfattende oversikt over hvilke type data som skal lagres etter direktivet. Etter art. 5 bokstav a skal de data som er nødvendig for å spore og identifisere kilden til en kommunikasjon lagres. Ved bruk av mobil- eller fasttelefon betyr det at A-nummeret, det vil si oppringers telefonnummer, samt navn og adresse på abonnenten eller den registrerte bruker lagres.Ved internettbruk, herunder e-post og IP-telefoni, skal tildelt brukeridentitet, den brukeridentitet og det telefonnummer som en kommunikasjon gjennom et offentlig telenett er tildelt lagres. Videre skal navn og adresse på den abonnent

---

[70] Walden (2009) s. 602

[71] Working Party on the Protection of Individuals with regard to the processing of Personal Data, arbeidsgruppe nedsatt etter art. 29 i direktiv 95/46/EF som fungerer som et uavhengig EU-rådgivningsorgan for personvernspørsmål og består av repesentanter fra alle EUs medlemsland. Datatilsynet har deltatt som observatør i organet, jfr. Datatilsynet, *Internasjonalt arbeid*

[72] Art. 29 WP 113 (2005) s. 2 og 7, Art. 29 WP 119 (2006) s. 3

[73] Art. 29 WP 113 (2005) s. 7, Art. 29 WP 119 (2006) s. 3

[74] Se forklaring av trafikk- og lokasjonsdata under punkt 1.3

eller registrerte bruker som en IP-adresse, brukeridentitet eller telefonnummer var tildelt på tidspunktet for kommunikasjonen lagres. Ved begrensningen til det som inngår i et offentlig telefonnett vil eventuell kommunikasjon i et lukket nett være unntatt fra lagringsplikten i datalagringsdirektivet.

Etter art. 5 bokstav b skal data som er nødvendig for å fastslå en kommunikasjons bestemmelsessted lagres. Det betyr at såkalte B- og C-nummer skal lagres. B- og C-nummer er telefonnumre til henholdsvis den som blir oppringt og nummer til en eventuelt videresendt abonnent, samt navn og adresse på abonnenten(e) eller de(n) registrerte bruker(e). Ved internettbruk skal brukeridentitet eller telefonnummer på den mottaker en IP-telefonsamtale er rettet mot lagres, samt dennes navn og adresse.

Bokstav c sikrer lagring av data som angir tidspunktet for kommunikasjonen. Ved fast- eller mobiltelefoni skal start og sluttidspunkt for samtalen lagres. Ved bruk av Internett skal dato og klokkeslett for av- og pålogging lagres sammen med IP-adressen kommunikasjonen er tildelt, uavhengig av om denne er fast eller dynamisk, samt brukeridentitet på abonnenten. I tillegg skal dato og klokkeslett for inn- og utlogging av e-post- og telefonitjenester på Internett lagres.

Bokstav d bestemmer at den anvendte telefon- eller internettjeneste skal lagres for å kunne identifisere hvilken type kommunikasjon som er benyttet.

Videre skal det lagres data for å identifisere hvilket kommunikasjonsutstyr som er benyttet, jfr. bokstav e. For fasttelefoni vil det si oppringers og mottakers telefonnummer, det samme som lagres etter bokstav a og b. For mobiltelefoni skal det foruten å lagre A- og B-nummeret også lagres A- og B-abonnentens IMSI[75]- og IMEI[76]-nummer. Det vil si en internasjonal mobilabonnentidentitet og internasjonalt mobilutstyrsidentitet. Enkelte tjenester er anonyme og forhåndsbetalte. For disse tjenestene skal dato og tidspunkt for

[75] IMSI: International Mobile Subscriber Identity

[76] IMEI: International Mobile Equipment Identity

første aktivering av tjenesten, en lokaliseringskode og fra hvor aktiveringen ble foretatt lagres. Ved internettilgang via oppringning skal oppringers telefonnummer lagres. Ved internettilgang via bredbånd skal endepunktet for kommunikasjonens opprinnelsesperson lagres.

Endelig skal lokasjonsdata ved bruk av mobilt utstyr lagres, jfr. bokstav f. Det vil si lokaliseringskoden ved kommunikasjonsstart samt data som viser hvor det mobile utstyret geografisk befinner seg i den periode det lagres trafikkdata.

Artikkel 5 annet ledd slår fast at direktivet ikke hjemler lagring av innholdsdata. Innholdsdata er blant annet hvilke internettsider som besøkes når en er oppkoblet til Internett. Når direktivet ikke hjemler lagring av innholdsdata vil det si at dersom en benytter en internettbasert e-posttjeneste, som for eksempel hotmail eller gmail, vil det ikke være mulig å lagre opplysinger om hvem som er sender og mottaker av en e-post i medhold av direktivet.[77] Kommunikasjonsløsninger som Skype og MSN er applikasjoner som ikke er definert som offentlige ekomtjenester vil heller ikke omfattes av datalagringsdirektivet.[78]

Relevante kommunikasjonsdata som kommer som følge av mislykkede oppringninger eller mislykkede påloggінger skal også lagres. Derimot skal det ikke lagres data tilknyttet oppringninger eller påloggingsforsøk som ikke oppnår forbindelse med det oppringte nummer.[79]

3.3 Lagringstid

Direktivets art. 6, som bestemmer lagringstid, åpner for en viss frihet for medlemslandene. Dataene skal lagres i minst seks måneder og maksimalt to år. Det vil si at det blir opp til norske myndigheter å bestemme en nærmere lagringstid. Det er foreløpig ikke tatt noen

[77] Samferdselsdepartementets høringsnotat s. 32

[78] Samferdselsdepartementets høringsnotat s. 32

[79] Samferdselsdepartementets høringsnotat s. 31

avgjørelse på hvor lang lagringstid som er ønsket i Norge. I høringsnotatet fra Samferdselsdepartementet er det uttalt at hvor lenge man skal lagre data ved en eventuell implementering av direktivet beror på en avveining mellom hensynet til kriminalitetsbekjempelse og hensynet til personvernet.[80] Departementet mener at lik lagringstid i de nordiske land vil være hensiktsmessig, men at lagringstid i de øvrige nordiske land likevel ikke er avgjørende for hva en faller ned på i Norge. Foreløpig er det bare Finland og Danmark av de nordiske landene som har implementert direktivet. Der har man valgt ett års lagringstid. Enkelte land har valgt ulik lagringstid for ulike tjenester som for eksempel i Storbritannia hvor det i den eksisterende bransjebaserte ordningen er ett års lagringstid for fast- og mobiltelefoni og seks måneder for lagring av data knyttet til Internett og e-postbruk.[81] I høringsnotatet kommer det frem at norske myndigheter i utgangspunktet ikke ønsker en delt lagringstid avhengig av hvilke teknologi som benyttes, men at det er ønskelig med tilbakemelding fra de ulike høringsinstansene om hva de tenker om problemstillingen. Hvor lang lagringstid det eventuelt vil bli i Norge synes derfor å være ganske uavklart. Ut fra hensynet til personvernet er det etter min mening best med en kortest mulig lagringstid.

3.4 Utlevering av lagrede data

Utlevering av de lagrede dataene er regulert i datalagringsdirektivet art. 4. Det er opp til hver enkelt medlemsstat å sikre at de lagrede data kun utleveres til kompetente myndigheter, i konkrete saker og i overenstemmelse med nasjonal rett, jfr. art. 4. Medlemsstatene er videre forpliktet til å lovfeste betingelser knyttet til utlevering. Statene plikter å påse at utlevering av data er i tråd med kravene til nødvendighet og proporsjonalitet som følger av internasjonale regler, herunder EMK. Politiet vil derfor ikke ha mulighet til en generell utlevering av lagrede trafikk- og lokasjonsdata.[82]

---

[80] Samferdselsdepartementets høringsnotat s. 39

[81] Samferdselsdepartementets høringsnotat s. 42

[82] Bignami (2007) s. 252 og Samferdselsdepartementets høringsnotat s. 60

4 EMK art. 8

4.1 Innholdet i EMK art. 8

EMK skal sikre enhver visse rettigheter og friheter, jfr. EMK art. 1. Etter menneskerettsloven § 2 første ledd gjelder EMK som norsk rett og skal ved motstrid gå foran annen lovgivning, jfr. § 3. EMK art. 8 er dermed å anse som preseptorisk lovgivning i Norge.

Bestemmelsene i EMK skal tolkes i lys av konvensjonspraksis fra den Europeiske Menneskerettsdomstolen. Dette er fordi en del av begrepene som er brukt i EMK ikke tar hensyn til rekkevidden av liknende begreper i hver enkelt konvensjonsbundet stat.

EMK art. 8 hjemler plikten til å respektere en rekke personlige interesser. I forhold til denne bestemmelsen har EMD vært tilbøyelige til en vid tolkning av definisjonen av hvilke rettigheter som er beskyttet. Dette har resultert i at omfanget av beskyttede rettigheter i art. 8 har økt og at den nå også dekker hemmelig overvåkning og fangers rettigheter, for å nevne noen.[83]

Artikkel 8 er bygd opp med en to ledds struktur. Første ledd fastslår selve rettigheten, respekt for privatlivet, mens andre ledd åpner for fravikelse av første ledd under visse vilkår.

4.2 EMK art. 8 første ledd

Første ledd i art. 8 bestemmer at *"everyone has the right to respect for his private and family life, his home and his correspondence"*. Ingen av de fire interessene: privatliv,

[83] Harris (2009) s. 361

familieliv, hjem eller korrespondanse, er fullt ut selvforklarende i seg selv og må derfor tolkes. De er alle uavhengige, slik at EMD på ingen måte er bundet av noen nasjonal fortolking av den enkelte interesse.[84] EMD har som regel brukt art. 8 første ledd på enkeltstående fakta i enkeltsaker og unngått en generell definisjon på hva hver enkelt av interessene skal innebefatte. Ved å unngå denne konkretiseringen har det vært mulig å utvikle regelen i samsvar med den generelle samfunnsutviklingen som har funnet sted. Likevel kan en si at retten til privatliv i form av retten til å leve uforstyrret og å ha sine private hemmeligheter er en underliggende verdi.

Første ledd i EMK art. 8 hjemler statens positive forpliktelse til å sikre sine borgere rett til respekt for sitt privatliv, familieliv, hjem og sin korrespondanse.[85] For å oppfylle sin positive forpliktelse må staten både sørge for å ha et lovverk som sikrer rettighetene og også legge til rette for utøvelsen av disse.[86]

Ved tolkningen av hva som ligger i de ulike interessene som er omfattet av EMK art. 8 har jeg valgt å fokusere på ”private life”, ”home” og ”correspondance”, ettersom lagring av trafikkdata kan tenkes å gå innunder et av disse alternativene.

4.2.1 ”Private life”

Med uttrykket *”right to respect for”* er det er respekten for de fire interessene som er beskyttet og ikke interessene i seg selv. *”Private life”* eller privatliv er et uttrykk som språklig favner vidt. Det må imidlertid vurderes hva som inngår i uttrykket i EMK. Er det en innsnevret form for ”privatliv” som kun omfatter den enkelte person, og i så fall hvilke deler av ens person, eller er uttrykket ment å favne videre? Som nevnt har ikke EMD gitt noen konkret forklaring på hva som er ment å inngå i begrepet, men praksis viser at *”private life”* er et vidt begrep. I saken Von Hannover v. Germany (2004) gjentar EMD at

[84] Harris (2009) s. 361

[85] Bygrave (1998) s. 257

[86] Ruiz (1997) s. 138

begrepet ”privatliv” også omfatter aspekter rundt personlig identitet, samt at det inkluderer en persons fysiske og psykiske integritet.[87] I Peck v. United Kingdom (2003) uttaler domstolen at *”private life”* i art. 8 og omfatter retten til personlig utvikling.[88] I Halford v. United Kingdom (1997) uttaler EMD i avsnitt 44 at det må være klart at telefonsamtaler gjort fra arbeidsplassen på samme måte som telefoner hjemmefra må anses å gå under begrepet ”privatliv” i EMK art. 8 første ledd. I PG and JH v. United Kingdom (2001) ble det uttalt at også etablering og utvikling av bekjentskap med andre mennesker og kontakt med omverdenen går innunder uttrykket ”privatliv” i art. 8.[89] Dette er også tilfellet selv om det finner sted i en offentlig sammenheng.[90]

Kjernen i innholdet av ”private life” er oppfatningen av den privates sfære som ingen andre har rett til å forstyrre. Det har de seneste tiårene vært en del saker som har slått fast at forstyrrelse i form av bråk fra nærliggende fabrikker og flyplasser medfører ulemper for den enkelte.[91] Kanskje er det ikke lenger bare de fysiske ulempene som er bakgrunnen for disse sakene, men også et ønske om ens rett til å være alene, å ha sitt eget private uforstyrrede rom.

Spørsmål knyttet til telefonavlyttning og lagring av trafikkdata kan nok tolkes inn i begrepet *”private life”*, men hører kanskje vel så gjerne under begrepene *”home”* eller *”correspondence”.*

4.2.2 ”Home”

Begrepet *”home”* kan tidvis virke vanskelig å definere. I saken Giacomelli v. Italy (2006) ble det uttalt at et hjem vanligvis må forstås som det fysiske området hvor privatliv og

---

[87] Avsnitt 50

[88] Avsnitt 57

[89] Avsnitt 56

[90] Von Hannover v. Germany (2004) avsnitt 50

[91] Rt. 2006 s. 486 (Gardermoen), Rt. 1982 s. 588 (Kjevikdommen), Rt. 1964 s. 609 (Hunton bruk) og Høstmælingen (2003) s. 228

familieliv normalt utøves.[92] Videre ble det uttalt at retten til respekt for sitt hjem ikke bare gir rett til det konkrete fysiske området, men også en rett til å nyte sitt hjem i ro og fred. Forstyrrelser som gjør at en ikke lenger kan nyte hjemmets fasiliteter kan være brudd på retten til respekt for sitt hjem. Et eksempel kan være at uvedkommende bryter seg inn i huset ditt eller at utbygging i nærheten gjør at livskvaliteten forringes. I Niemietz v. Germany (1992) ble det i avsnitt 30 slått fast at en utvidende tolkning av "home" til å også gjelde ens arbeidsplass er fullt forenlig med den franske teksten hvor ordet "domicile" er brukt. Både den franske og den engelske teksten er offisielle versjoner av EMK slik at EMD kan legge begge versjonene til grunn for sine tolkninger.

4.2.3 "Correspondence"

Endelig beskytter EMK retten til respekt for korrespondanse. I den engelske versjonen er ordet *"correspondence"* benyttet. Med rett til respekt for ens korrespondanse menes at vi har en ubetinget rett til usensurert og uforstyrret kommunikasjon med andre mennesker.[93] Tradisjonelt har korrespondanse vært forstått som brevpost, men også på dette området har det vært en viss samfunnsutvikling. I Klass and Others v. Germany (1978) ble telefonsamtaler innfortolket i begrepet *"correspondence"*.[94] Dette er fulgt opp av EMD i blant annet Malone v. United Kingdom (1984), avsnitt 64, og Halford v. United Kingdom (1997), avsnitt 44. I Copland v. United Kingdom (2007), avsnitt 41, kom EMD til at *"correspondence"* må tolkes utvidende til og å omfatte e-post og bruk av Internett. På denne måten har EMK art. 8 klart å holde tritt med den teknologiske utviklingen.

EMD vurderte trafikkdata opp mot EMK art. 8 for første gang i Malone v. United Kingdom (1984). Saksøker hadde da vært utsatt for både telefonavlytting og såkalt "metering" fra politiet. "Metering" er en metode for å oppfange og lagre opplysninger som trafikkdata. I denne sak hadde "metering" skjedd ved at politiet brukte en slags enhet som

[92] Avsnitt 76

[93] Ruiz (1997) s. 138

[94] Avsnitt 41

automatisk lagret alle telefonnumre sakssøker ringte. Domstolen la vekt på at slike trafikkdata som ble fanget opp ved nevnte metode var å anse som en sentral del av telekommunikasjon og at utlevering av slike data uten abonnentens viten utgjorde et brudd på rettighetene i EMK art. 8.[95]

Et spørsmål er hva som skjer når brevet eller e-posten har blitt sendt fra avsender. Når brevet er kommet frem til mottaker har ikke avsender lenger noen rett til respekt for sin korrespondanse. En kan heller ikke si at EMK art. 8 er krenket om den annen part i en telefonsamtale videreforteller innholdet av en samtale til en tredjeperson.[96] I enkelte kommunikasjonslinjer kan det likevel være en forventning om taushetsplikt, for eksempel ved samtaler mellom advokat og klient eller mellom helsepersonell og pasient. Dette gjør at man ikke uforbeholdent kan legge til grunn at enhver står fritt til å viderefortelle innholdet av en telefonsamtale, e-post eller liknende. I tillegg kan andre normer og regler fastsette taushetsplikt for mottaker.

Et kanskje vel så viktig spørsmål er hvilken alvorlighetsgrad en overtredelse må ha for at et brudd på EMK art. 8 første ledd skal konstateres i forhold til korrespondansebegrepet. Spørsmålet kommer typisk opp i sammenheng med friheten til å kommunisere, men kan ifølge Ruiz vel så gjerne utvides og bli brukt på retten til hemmeligholdelse rundt ens telekommunikasjon, herunder telefon, e-post og internettbruk.[97] I begynnelsen av EMKs virketid måtte det nærmest et totalforbud mot kommunikasjon til for å konstatere et brudd på EMK art. 8 første ledd. Ble en form for kommunikasjon forbudt ville ikke det utgjøre et inngrep ettersom øvrige former for kommunikasjon fortsatt ville være tillatt.[98] Dette ble imidlertid endret gjennom EMDs praksis på 1970-tallet. Da kom domstolen til at retten til respekt for sin korrespondanse i art. 8 forutsatte en fri flyt av kommunikasjon. [99] Dette har

---

[95] Malone v. United Kingdom (1984) avsnitt 84

[96] Harris (2009) s. 381 og Ruiz (1997) s. 137

[97] Ruiz (1997) s. 137

[98] Ruiz (1997) s. 137

[99] Silver and Others v. United Kingdom (1983), report of the Commission, avsnitt 270

medført at sensur eller annen aktiv begrensning i denne frie flyten av kommunikasjon kan bli ansett som et inngrep i eller brudd på retten til respekt for sin korrespondanse.[100] I den positive dimensjonen er en stats forpliktelser begrenset til å ta forholdsregler og fjerne hindringer for utøvelsen av retten såfremt hindringene ikke er i samsvar med EMK art. 8 annet ledd.

4.2.4 Oppsummering

Oppsummeringsvis kan man si at de viktigste vurderingstemaene for å avgjøre om det foreligger et brudd på EMK art. 8 første ledd i relasjon til personvernet, er hvilken type opplysninger det er snakk om, på hvilken måte de er behandlet og i hvilken sammenheng opplysningene er behandlet.[101] Antakelig vil opplysninger som avslører detaljer om den registrertes personlighet uten at vedkommende er klar over det anses som et inngrep i rettighetene etter art. 8 når opplysningene er egnet til å sette personen i et dårlig lys.[102]

Grensen mellom hva som dekkes av begrepet *"correspondence"* og hva som går innunder *"private life"* er flytende, da de to interessene til dels er overlappende. En kan tenke at en advokat som bryter taushetsplikten ved å viderefortelle innholdet fra en telefonsamtale med en klient har brutt både klientens rett til respekt for privatliv og klientens rett på respekt for korrespondanse. Ulovlig overvåking av telefonsamtaler er også et tilfelle som dekkes av begge begrepene.

Som redegjort for over er det retten til respekt for de nevnte interesser EMK art. 8 beskytter og ikke interessene i seg selv. Bestemmelsen favner ganske vidt slik at deler av den vanlige myndighetsøvelsen ofte vil tangere bestemmelsens første ledd. Lovgivning rundt familieliv vil kunne tenkes å være på grensen mot hva som er tillatt under respekt for familieliv, og reglene i straffeprosessloven om kommunikasjonskontroll grenser mot både respekt for

---

[100] Ruiz (1997) s. 138

[101] Bygrave (1998) s. 269

[102] Bygrave (1998) s. 269

privatliv og respekt for korrespondanse. Ved å bruke ordet *"respect"* i art. 8 første ledd har man utvidet omfanget av EMK art. 8 til å favne videre enn kun beskyttelse av selve rettigheten.

4.3 EMK art. 8 annet ledd

I EMK art. 8 annet ledd står det: *"There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."*

Denne bestemmelsen gir myndighetene en mulighet til å gripe inn i rettighetene en person har etter EMK art. 8 første ledd. Som regel blir det ikke spørsmål om hvorvidt myndighetsutøvelsen strider mot rettighetene i første ledd, men heller om den kan være berettiget etter andre ledd. EMK art. 8 annet ledd oppstiller visse vilkår som må være oppfylt for at myndighetene skal kunne gripe inn i rettighetene etter første ledd. En eventuell inngripen må være lovfestet, den må ha et legitimt formål og den må være nødvendig i et demokratisk samfunn.

"In accordance with the law" betyr at inngrep må være i samsvar med lov. Det er også et krav om at loven må være tilstrekkelig klar og konkret.[103] Dette vilkåret har vært særlig viktig i saker om telefonavlytting og hemmelig overvåking. I Malone v. United Kingdom (1984) uttalte domstolen at kravet om at loven må være tilstrekkelig klar og tydelig er spesielt viktig i saker hvor myndighetene har mulighet til å ty til et så alvorlig inngrep som overvåking.[104]

[103] Harris (2009) s. 400

[104] Avsnitt 67

Når det kan slås fast at et inngrep i EMK art. 8 er i tråd med andre lovregler har EMD vurdert hvorvidt det foreligger et legitimt formål. Etter EMK art. 8 annet ledd vil legitimerte formål være når noe er av interesse for nasjonens sikkerhet, offentlig trygghet eller landets økonomiske velferd. Dette gir en videre adgang til inngrep enn i EMK art. 9 til 11, hvor økonomisk velferd ikke er tilstrekkelig for å gripe inn i rettighetene. Videre vil inngripen med formål å forebygge kriminalitet, å beskytte helse eller moral eller for beskyttelse av andres rettigheter og friheter være tillatt. Disse seks nevnte formål er alternative.

Endelig er det et krav om at en inngripen må være nødvendig i et demokratisk samfunn. Det er ikke tilstrekkelig at en stat har en eller annen grunn til å gripe inn i rettighetene etter EMK art. 8, grunnen må være "nødvendig". "Nødvendig" er også et skjønnsmessig begrep og det kan oppstå tvil om hva som egentlig menes med det. Uttrykket *"necessary in democratic society"* går igjen i art. 8 annet ledd til 11 annet ledd og kan forstås på samme måte i de nevnte bestemmelser. I saken Handyside v. United Kingdom (1976) uttalte EMD at statlige myndigheter nok var nærmere til å gi en eksakt definisjon av hva som ligger i uttrykket *"necessary"* enn det domstolen var, men de kom likevel med noen føringer på hva som ligger i uttrykket. De uttalte i nevnte sak at selv om "necessary" ikke må forstås like snevert som "absolutt nødvendig" i art. 2 annet ledd eller "strengt nødvendig" i art. 6 første ledd, er det heller ikke like vidt som uttrykkene "vanlig" i art. 4 tredje ledd bokstav a eller "rimelig" i art. 5 tredje ledd.[105] Dermed utelukket man overdrevent snevre eller svært vide fortolkninger av begrepet. Senere så EMD behovet for proporsjonalitet. I Olsson v. Sweden (1988) uttalte retten at om man så på domstolens tidligere praksis vil nødvendighetsbegrepet i EMKs forstand innebære at inngrep i rettighetene må korrespondere med et presserende samfunnsbehov og det må stå i forhold til det legitimerte formålet med inngrepet. Videre ble det uttalt at domstolen vil ta hensyn til at statene selv har en viss skjønnsmargin ved vurderingen av nødvendighetsbegrepet.[106]

[105] Handyside v. United Kingdom (1976) avsnitt 48

[106] Avsnitt 67

For at en stat skal kunne gripe inn i rettighetene EMK art. 8 er ment å beskytte må staten kunne bevise at en inngripen som begrenser saksøkers rettigheter etter EMK art. 8 første ledd er nødvendig ut fra et presserende samfunnsbehov. EMD har erkjent at enkelte aspekter ved rettighetene i EMK art. 8 er viktigere enn andre. Jo mer dyptgående en inngripen er, jo større rettferdiggjøring kreves for at den skal være i tråd med art. 8.

Ved vurdering av forholdsmessigheten har statene en viss skjønnsmargin.[107] Dette kom frem i Klass and Others v. Germany (1978). EMD understreket i denne saken imidlertid at skjønnsmarginen på ingen måte er ubegrenset og at en stat ikke står fritt til å iverksette ethvert tiltak for å bekjempe terrorisme.[108] Hos Yourow er statenes skjønnsmargin definert som et slags "albuerom"; en handlefrihet for statene.[109] Skjønnsmarginen kan begrunnes med at hva som må til for å oppfylle et nødvendighetskrav kan variere fra stat til stat og at den enkelte stat er nærmest til å vurdere nødvendighetskravet.[110] Omfanget av skjønnsmarginen vil variere avhengig av hva slags inngrep det er snakk om og hvilke rettigheter det gjøres inngrep i.[111] For eksempel har statene en vid skjønnsmargin når formålet med inngrepet er å sikre den nasjonale sikkerhet.[112] Videre vil skjønnsmarginen utvides på områder hvor det ikke foreligger en felles rettsenhet i Europa.[113]

[107] Yourow (1996) s. 2

[108] Avsnitt 49

[109] Yourow (1996) s. 13

[110] Janis, Kay og Bradley (2009) s. 242

[111] Høstmælingen (2003) s. 124 og Leander v. Sweden (1987) avsnitt 59

[112] Høstmælingen (2003) s. 223 og Leander v. Sweden (1987) avsnitt 67

[113] Høstmælingen (2003) s. 221 og 255

5 Kriminalitetsbekjempelse på bekostning av personvernet?

5.1 Vil lagring av trafikkdata stride mot respekten for privatliv og korrespondanse?

Lagring av trafikkdata er noe som berører alle borgere i en betydelig grad. Fri kommunikasjon er en av grunnpilarene i et demokratisk samfunn, og er blant annet beskyttet gjennom EMK art. 8.

Retten til uforstyrret telekommunikasjon er ikke bare dekket av alternativet *"the right to respect for (...) correspondence"* i EMK art. 8, men kan også omfattes av alternativet *"private life"*, jfr. punkt 4.1.1 ovenfor. EMD har konkludert med at korrespondansebegrepet omfatter telekommunikasjon[114] og internettbruk, herunder e-postkorrespondanse[115].

For at noe skal kunne falle inn under begrepet *"private life"* i EMK art. 8 må det være et visst element av privatlivet som blir berørt. En person bør ha rimelig grunn til å anta at sine personlige telefonsamtaler og internettbruk er av såpass privat karakter at *"right to repect for private life"* også omfatter privat telekommunikasjon.

Etter datalagringsdirektivet art. 5 annet ledd skal ikke innholdsdata lagres. Spørsmålet er om en omfattende adgang til lagring av trafikkdata kan sies å stride mot EMK art. 8 første ledd.

Datalagringsdirektivet vil pålegge private aktører å lagre trafikkdata for en eventuell senere utlevering til politi og påtalemyndighet. Dette kan tenkes å stride mot EMK art. 8, noe også

[114] Klass and Others v. Germany (1978) avsnitt 41

[115] Copland v. United Kingdom (2007) avsnitt 41

Personvernkommisjonen nevnte i sin utredning.[116] EMD behandlet et liknende spørsmål om innhenting av trafikkdata i saken Malone v. United Kingdom (1984) og kom til at slik innhenting må anses som et brudd på EMK art. 8 første ledd, uavhengig av formålet og omstendighetene rundt, med mindre det blir rettferdiggjort etter EMK art. 8 annet ledd. Domstolen la blant annet vekt på at trafikkdata er et nødvendig element i telekommunikasjon.[117] I Leander v. Sweden (1987) konkluderte EMD med at både lagring og utlevering av informasjon knyttet til Torsten Leanders privatliv var å anse som et brudd på EMK art. 8 første ledd.[118] Disse avgjørelsene taler for at lagring slik det er foreskrevet i datalagringsdirektivet er i strid med EMK art. 8 første ledd, da direktivet pålegger lagring av data av en slik art som må anses å være en del av ens privatliv.

Generelt er innhenting og lagring av personopplysninger ansett som et alvorlig inngrep i en persons private sfære. Art. 29 WP mener lagring av trafikkdata vil krenke retten til fortrolig kommunikasjon som er hjemlet i EMK art. 8.[119]

Datalagringsdirektivet pålegger lagring av hvor en befinner seg ved telefonsamtalens start. samt hvem som ringer hvem til enhver tid. Analyser av slike opplysninger kan avsløre detaljer rundt en persons politiske, finansielle, seksuelle eller religiøse preferanser,[120] dette er å anse som sensitive personopplysninger[121] og må også ses som inngrep i retten til respekt for privatlivets fred.

Det kan også stilles spørsmål ved hvordan opplysningene skal lagres. I Samferdselsdepartementets høringsnotat er det skissert to mulige løsninger i forhold til lagringssted, enten at trafikkdataene lagres hos tilbyder eller at opplysningene lagres i en

---

[116] NOU 2009:1 s. 191

[117] Malone v. United Kingdom avsnitt 84

[118] Avsnitt 48

[119] Art. 29 WP 113 (2005) s. 3

[120] Breyer (2005) s. 365

[121] Popplyl. § 8 nr. 8

sentral database. Departementet har av personvernmessige hensyn ikke foreslått en løsning med sentral lagring av opplysningene.[122] Dette er i tråd med signaler fra Datatilsynet. Art. 29 WP har uttalt at det er viktig å skille mellom dataene som skal lagres i medhold av datalagringsdirektivet og de data som en teletilbyder lagrer for andre formål, som fakturering, for å sikre at tilbyderne ikke bruker data lagret i medhold av datalagringsdirektivet til egen bruk.[123] En løsning med et slikt skille er støttet av både Datatilsynet og ekomtilbydere og anbefalt av art. 29 WP.[124] Direktivet har ikke noe krav om at opplysningene skal lagres atskilt, men de nødvendige tekniske og organisatoriske løsninger må være på plass for å opprettholde datasikkerheten.[125]

Samferdselsdepartementet har i sitt høringsnotat i anledning direktiv 2006/24/EF lagt til grunn at datalagringsdirektivet medfører et inngrep i rettighetene etter EMK art. 8 første ledd.[126] Det samme synspunktet støttes av Wessel-Aas og Bruce.[127]

5.1.1 Rettspraksis knyttet til datalagringsdirektivet

Datalagringsdirektivet har ikke vært oppe til vurdering hos EMD enda, men direktivet har vært til vurdering i nasjonal domstol i Romania og Tyskland. I Romania ble det avsagt dom i forfatningsdomstolen 8. oktober 2009 som fastslo at implementeringen av direktivet i rumensk rett strider mot art. 26, 28 og 30 i den rumenske grunnloven.[128] Artikkel 28 i den rumenske grunnloven bestemmer at:*"the secrecy of letters, telegrams, and other postal communications, of telephone conversations, and of any other legal means of communication is inviolable"*

---

[122] Samferdselsdepartementets høringsnotat s. 35

[123] Samferdselsdepartementets høringsnotat s. 36

[124] Art. 29 WP 113 (2005) s. 8

[125] Datalagringsdirektivet art. 7

[126] Samferdselsdepartementets høringsnotat s. 27

[127] Wessel-Aas (2010) s. 51 og Bruce (2010) s. 9

[128] Romania Constitutional Court, Decision no. 1258, 08.10.2009

Artikkel 26 lyder: *"(1) The public authorities shall respect and protect the intimate, family and private life.*
(2) Any natural person has the right to freely dispose of himself unless by this he infringes on the rights and freedoms of others, on public order or morals." [129]

Bestemmelsene i den rumenske konstitusjonen som var oppe til vurdering i den rumenske forfatningsdomstolen beskytter de samme interesser som EMK art. 8.

En liknende sak var opp i den tyske forfatningsdomstolen som 2. mars 2010 slo fast at Tysklands implementering av datalagringsdirektivet strider mot den tyske grunnloven.[130] Avgjørelsen var ikke enstemmig. På spørsmålet om implementeringen var grunnlovstridig var det to dissenterende dommere, hvorav én av de to også dissenterte på spørsmålet om implementeringen var i strid med tysk materiell lov. Det er verdt å merke seg at det var selve implementeringen som ble ansatt forfatningsstridig, ikke datalagring i seg selv.[131]

Selv om datalagringsdirektivet må anses å stride mot retten til respekt for privatlivet og korrespondanse kan et slikt inngrep være lovlig dersom vilkårene i EMK art. 8 annet ledd er oppfyllt.

5.2 Proporsjonalitetsprinsippet

EMK art. 8 andre ledd hjemler inngrep i retten til respekt for privatliv og korrespondanse dersom det er i samsvar med lov og er nødvendig i et demokratisk samfunn av hensyn til den nasjonale sikkerhet eller for å forebygge kriminalitet og uorden. Ulempene datalagringsdirektivet medfører må dermed måles opp mot formålet med direktivet for å avgjøre om det kan sies å være et forholdsmessig inngrep. Det må ses på forventet effekt av

[129] Constitution of Romania art. 26, art. 28

[130] Datatilsynet, *forfatningsstridig datalagring i Tyskland*

[131] Press release, Federal Constitutional Court of Germany, s. 3 og 4

utvidet lagring av trafikkdata i forhold til den ulempene det kan medføre for borgerne, samt foretas en proporsjonalitetsvurdering.
For at proporsjonalitetskravet slik det er kommet til uttrykk i EMK art. 8 annet ledd skal oppfylles må et inngrep i rettighetene hjemlet i første ledd oppfylle tre vilkår: lovskravet, formålskravet og kravet om forholdsmessighet.

Først vil lovskravet drøftes. Deretter vil formålskravet bli gjennomgått. Til slutt vurderes forholdsmessigheten i punkt 5.2.3.

5.2.1 Kort om lovskravet

En inngripen i rettighetene i EMK art. 8 første ledd må være i samsvar med lov, jfr. *"in accordance with the law"* i EMK art. 8 annet ledd. Ved en eventuell implementering i Norge må direktivet gjøres til norsk lov gjennom transformasjon (gjengivelsesmetoden) eller inkorporasjon (henvisningsmedtoden).[132] Direktivet vil da bli å anse som norsk lov og gjelde på lik linje med øvrige norske lover.

I forhold til EMK er det et krav at nasjonale regler er tilgjengelige og forutberegnelige for borgerne.[133] Hva som ligger i lovskravet har vært vurdert av EMD flere ganger. I saken Malone v. United Kingdom (1984) uttalte domstolen at uttrykket *"in accordance with law"* skal tolkes i lys av prinsippene fra avgjørelsen Sunday Times v. United Kingdom (1979). I sistnevnte avgjørelse var det uttrykket *"prescribed by law"* i EMK art. 10 som ble fortolket. Der ble det slått fast for det første at det ordet *"law"* ikke bare sikter til skriftlige lover, men også uskreven rett (*"unwritten law"*).[134] Ordet *"law"* fordrer likevel at en regel er tilstrekkelig klart og presist formulert slik at borgerne klarer å innrette seg etter den, og at de skal kunne forutse hvilke konsekvenser det kan få å ikke følge gjeldene regler.[135]

---

[132] Ruud og Ulfstein (2002) s. 36

[133] Bruce (2010) s. 10

[134] Sunday Times v. United Kingdom (1979) avsnitt 47

[135] Silver and Others v. United Kingdom (1983) avsnitt 88

Videre må det inngrepet det er tale om ha et visst grunnlag i nasjonal rett.[136] I Silver and others v. United Kingdom (1983) uttalte domstolen at lovverket også må være tilgjengelig for innbyggerne slik at de har tilstrekkelig oversikt over hvilke lovregler som gjelder på et bestemt område.[137]

Fra samferdselsdepartementet er det foreslått følgende tillegg til dagens ekomlov § 2-8: *"Tilbyder som nevnt i første ledd skal lagre trafikkdata, lokaliseringsdata og data nødvendig for å identifisere abonnenten eller brukeren i X måneder for å legge til rette for etterforskning og rettsforfølgning av alvorlige straffbare forhold. Plikten etter første punktum gjelder data som genereres eller behandles i tilbyders elektroniske kommunikasjonsnett ved bruk av fasttelefoni, mobiltelefoni, internetttelefoni, internettaksess og e-post."*[138]

Uttrykket *"alvorlige straffbare forhold"* er ikke nærmere konkretisert i departementets forslag til endring i ekomloven. Det er derimot i forslag til endring i straffeprosessloven § 210 foreslått at utlevering av lagrede data som er lagringspliktige etter e-koml. § 2-8 kun skal skje når noen *"med skjellig grunn mistenkes for en handling eller forsøk på en handling som rammes av straffeloven §§ 91, 91a, 104a, 132b, 145 annet ledd, 145a, 162, 201a, 203, 204, 317, jf. §§ 162 eller 390a."*[139]

Således ser lovskravet i EMK art. 8 annet ledd ut til å være oppfyllt i forhold til Samferdselsdepartementets forslag. Dette synspunktet støttes også av Bruce.[140] Heller ikke Wessel-Aas tror lovskravet vil volde problemer i denne sammenheng.[141]

---

[136] Malone v. United Kingdom (1984) avsnitt 66

[137] Avsnitt 87

[138] Samferdselsdepartementets høringsnotat s. 59

[139] Samferdselsdepartementets høringsnotat s. 60

[140] Bruce (2010) s. 10

[141] Wessel-Aas (2010) s. 51

5.2.2 Formålskravet

For at et inngrep skal være legitimert etter EMK art. 8 annet ledd må det være gjort av hensyn til den nasjonale sikkerhet og offentlig trygghet eller for å forebygge kriminalitet eller uorden. Formålet med dataladringsdirektivet er å harmonisere medlemslandenes bestemmelser vedrørende tilbydere av offentlig kommunikasjoners plikt til å lagre trafikkdata i den hensikt å sikre at det er tilgang på slike opplysninger i forbindelse med etterforskning, avsløring og rettsforfølgning av alvorlig kriminalitet, jfr. direktivets art. 1. I den offisielle engelske versjonen er uttrykket *"serious crime"* brukt uten at det blir forklart nærmere. Det skal være opp til hvert enkelt medlemsland å definere hva som skal menes med *"serious crime"* i nasjonal lovgivning.[142] Norske myndigheter har foreløpig definert alvorlig kriminalitet som lovbrudd med strafferamme på fengsel i minst tre år eller handlinger som omfattes av nærmere angitte bestemmelser i straffeloven hvor trafikkdata er antatt å være effektivt i etterforskningen.[143] Eksempler på dette er hvitvasking (strl. § 317), narkotikaforbrytelser (strl. § 126) og visse forbrytelser mot sedelighet og rikets sikkerhet som i utgangspunktet har en lavere strafferamme enn tre år.[144]

Datatilsynet har stilt seg skeptisk til hvorvidt tiltak i medhold av datalagringsdirektivet vil være effektive og har lagt vekt på muligheten til å kunne komme seg unna lagringen[145] ved eksempelvis å benytte internettbaserte mailsystemer som hotmail eller gmail. Dette er fordi lagring av trafikkdata ved bruk av slike mailadresser vil medføre lagring av hvilke nettsider en har besøkt og dermed anses som innholdsdata som ikke kan lagres i medhold av direktivet.[146]

---

[142] Datalagringsdirektivets art. 1 første ledd

[143] Samferdselsdepartementets høringsnotat s. 54

[144] Samferdselsdepartementets høringsnotat s. 60

[145] Datatilsynets høringsuttalelse s. 7

[146] Datalagringsdirektivet art. 5 nr. 2

Begrepet *"serious crime"* har vært kritisert for å være for vagt angitt, blant annet av art. 29 WP som mente uttrykket burde defineres klart i direktivet.[147] I Norge har Datatilsynet uttalt at myndighetenes likestilling av alle lovbrudd med strafferamme på minst tre års fengsel ikke er forsvarlig. Dette er fordi en manglende klar definisjon av begrepet i praksis kan innebære at direktivet kan bli brukt mot gjentatte enklere lovbrudd som egentlig ikke er tilsiktet omfattet av direktivet.[148]

De legitimerte formål som er listet opp i EMK art. 8 annet ledd er relativt vidt formulert. Inngrep kan skje med "*hensyn til den nasjonale sikkerhet, offentlig trygghet eller (…) for å forebygge uorden eller kriminalitet"*. Dette gjør at formålskravet sjelden byr på problemer for statene.[149] Formålet med datalagringsdirektivet er å etterforske, avsløre og straffeforfølge *"serious crime,"* jfr. direktivets art. 1. Som nevnt under punkt 5.2.1 er *"serious crime"* oversatt med *"alvorlig straffbare forhold"* i Samferdselsdepartementets utkast til endring i dagens ekomlov. Dette må sies å være i samsvar med formålskravet i EMK art. 8 annet ledd.

5.2.3 Forholdsmessighet

Endelig må inngrepet oppfylle proporsjonalitetskravet i EMK art. 8 annet ledd. Proporsjonalitetskravet består av to deler. Den første delen er hvorvidt det finnes andre mindre byrdefulle løsninger for å oppfylle myndighetenes mål. Den andre delen er en vurdering av viktigheten av rettigheten opp mot det offentlige formålet.[150]

---

[147] Art. 29 WP 119 (2006) s. 3 og art. 29 WP 113 (2005) s. 7

[148] Datatilsynets høringsuttalelse s. 11 og Apenes (2010)

[149] Bruce (2010) s. 14

[150] Bignami (2007) s. 242

Proporsjonalitetskravet i EMK art. 8 annet ledd er formulert som *"necessary in a democratic society"*. I det ligger det at inngrepet må være begrunnet i et påtrengende samfunnsmessig behov og samtidig være forholdsmessig i forhold til formålet.[151]

I vurderingen av forholdsmessighet har EMD gitt statene en viss skjønnsmargin. Omfanget av denne vil variere med hvilken rettighet det gjøres inngrep i og hvilket formål som søkes oppfylt ved inngrepet.[152] EMD har uttalt at skjønnsmarginen vil innsnevres dersom interessen det er tale om er av avgjørende betydning for den enkeltes utbytte av intime eller viktige rettigheter.[153] Videre uttalte domstolen at skjønnsmarginen er bredere dersom det er uenighet mellom medlemslandene om betydningen av interessen som står på spill eller hvordan den best kan beskyttes.[154]

EMD har uttalt at EMK ikke må tolkes på en slik måte at politiets arbeid blir umuliggjort eller uvanlig byrdefull.[155]

Selv om datalagringsdirektivet innføres vil det være flere muligheter for å unndra seg lagring. Dette er særlig fordi innholdsdata ikke kan lagres, jfr. datalagringsdirektivets art. 5 andre ledd. Organiserte kriminelle kan velge å benytte seg av internettbaserte e-postløsninger, som gmail og hotmail, som ikke fanges opp av direktivet. Det er også utfordringer knyttet til internettbruk via internettkafeer eller offentlige bibliotek. Ved bruk av slike offentlige internettløsninger vil ikke trafikkdata lagret i medhold av direktivet avsløre identiteten til brukeren. Dermed forsvinner noe av hensikten med direktivet.

---

[151] Schartum og Bygrave (2004) s. 96, se forøvrig punkt 4.3

[152] Schartum og Bygrave (2004) s. 96 og Bruce (2010) s. 16

[153] S. and Marper v. United Kingdom (2008) avsnitt 102

[154] S. and Marper v. United Kingdom (2008) avsnitt 102

[155] Bing (2009) og K.U. v. Finland (2008) avsnitt 48

5.2.3.1 Er det behov for datalagringsdirektivet?

Datatilsynet har stilt spørsmål ved hvorvidt det er godtgjort at det er et slikt påtrengende samfunnsbehov for økt lagring av trafikk- og lokasjonsdata i forhold til hva det er mulighet til i dag.[156]

Som nevnt i oppgavens kapittel 2 lagres allerede noe trafikkdata. Til Samferdselsdepartementet har Post- og teletilsynet oppgitt at det de senere år har vært en markant økning i antall begjæringer fra politiet om innhenting av trafikkdata. Mens det i 2001 var 982 begjæringer har det økt til 1900 begjæringer i 2008.[157] Post- og teletilsynet har opplyst til Samferdselsdepartementet at begjæringene nesten utelukkende gjeder data i forhold til mobiltelefoner.[158] Det foreligger imidlertid ingen statistikk over hvor gamle opplysninger politiet har etterspurt.[159] Politiet etterspør i dag normalt ikke oppysninger som er eldre enn tre til fem måneder. Dette kan ha sammenheng med at politiet vet at tilbydere av elektronisk kommunikasjon per i dag ikke har anledning til å lagre data i et lengre tidsrom.[160] Ettersom data rundt internettbruk lagres i svært liten grad etterspør heller ikke politiet disse opplysningene i noen særlig grad.[161] Det er derfor svært lite statistikk over behovet og vanskelig å få oversikt over hvor påtrengende behovet for datalagring egentlig er. Tall fra Storbritannia viser at trafikkdata som er eldre enn seks måneder ofte har vært nyttig for politiet der i forbindelse med etterforskning av alvorlige forbrytelser.[162]

Videre kan lokasjonsdata være nyttig for etterforskning og straffeforfølgning. Lokasjonsdata viser hvor vedkommende som kommuniserte befant seg på et bestemt sted på et bestemt tidspunkt. Uavhengig av hvem personen kommuniserte med kan

---

[156] Datatilsynets høringsuttalelse s. 6

[157] Samferdselsdepartementets høringsnotat s. 18

[158] Samferdselsdepartementets høringsnotat s. 19

[159] Samferdselsdepartementets høringsnotat s. 39

[160] Samferdselsdepartementets høringsnotat s. 39

[161] Samferdselsdepartementets høringsnotat s. 19

[162] Bignami (2007) s. 247

opplysningen brukes som et bevis for hvor vedkommende oppholdt seg på lik linje med vitneobservasjoner.[163]

Et eksempel fra norsk strafferett på at trafikk- og lokasjonsdata har vært av betydning for bevisførselen finnes i en avgjørelse fra Borgarting lagmannsrett fra 2008.[164] I denne saken ble en person dømt til 15 års fengsel for overtredelse av strl. § 233 og § 268 jfr. § 267 for grovt ran og for å ha forvoldt en annen persons død. Her var telefonutskrifter som viste hvem tiltalte hadde ringt når og hvor mobilen hans da befant seg av avgjørende betydning for å få bevist faktum i saken.

Et moment ved vurdringen av behovet for datalagringsdirektivet er at utviklingen ser ut til å gå i retning av at man på sikt vil betale en fast sum for fri bruk av telefoni slik at teletilbyderne ikke lenger vil ha noen mulighet til å lagre trafikkdata av faktureringshensyn.[165] Da vil det ikke være noen mulighet for politiet til å hente inn trafikkdata knyttet til elektronisk kommunikasjon i etterkant ettersom opplysningene vil slettes umiddelbart, jfr. e-koml. § 2-7 annet ledd. Ved en slik utvikling vil datalagringsdirektivet være eneste måte å sikre politi og påtalemyndighet tilgang på historiske trafikkdata.

K.U. v. Finland (2008) er et annet eksempel på en sak hvor tilgang til trafikkdata var av avgjørende betydning. Saksforholdet gikk ut på at en ukjent person hadde lastet opp en kontaktannonse på Internett i navnet på en annen uvitende person. Fornærmede i saken var 12 år og ble først klar over annonsen da han fikk en e-posthenvendelse fra en mann som tilsynelatende svarte på annonsen. Kontaktannonsen inneholdt flere detaljerte opplysninger om gutten, blant annet fødselsdato, beskrivelse av utseendet hans og en link til guttens daværende hjemmeside, hvor man kunne se bilde av fornærmede. Faren til fornærmede krevde at politiet skulle identifisere personen som hadde lastet opp kontaktannonsen for å

[163] Willassen (2010) s. 5

[164] LB2008-61703 (Lovdata)

[165] Bruce (2010) s. 8

kunne straffeforfølge vedkommende. Internetttilbyderen nektet å utlevere informasjon om hvem som stod bak den dynamiske IP-adressen, og begrunnet dette med den lovfestede retten til respekt for korrespondanse.

Her stod to personvernhensyn mot hverandre. For det første hensynet til offerets personvern, som klart var blitt krenket da en annen person opprettet kontaktannonse i guttens navn uten guttens samtykke eller viten. For det andre er gjerningspersonen også beskyttet ut fra hensynet til personvernet gjennom EMK art. 8 og retten til respekt for sin korrespondanse; i det ligger også en rett til hemmeligholdelse av sin kommunikasjon.[166] EMD la i sin vurdering av disse hensyn vekt på at det var begått en kriminell handling mot en mindreårig person, og at handlingen som var begått kunne tenkes å gjøre fornærmede til et mål for pedofile personer. Retten uttalte at enhver bruker av tele- og internettjenester i utgangspunktet skal være garantert respekt for sitt eget privatliv.[167] I denne saken veide imidlertid hensynet til oppklaring av den kriminelle handling og mulighet for straffeforfølgelse av gjerningspersonen tyngst.

De to nevnte avgjørelser tyder på at det kan være et visst behov for datalagringsdirektivet selv om det ikke finnes noen oversikt over forventet behov for det i Norge.

Datalagringsdirektivet forbyr lagring av innholdsdata, som eksempelvis hvilke internettsider en besøker. For å fange opp trafikkdata, hvem som har kontaktet hvem når, fra kommunikasjonssystemer som eksempelvis gmail og Skype må innholdsdata lagres for å kunne bevise at person i det hele tatt har brukt tjenesten. Slike data vil derfor neppe kunne lagres i medhold av datalagringsdirektivet.

[166] Ruiz (1997) s. 147

[167] K.U. v. Finland (2008) avsnitt 49

5.2.3.2 EMD-praksis rundt datalagring og proporsjonalitet

5.2.3.2.1 Klass and Others v. Germany

Klass and Others v. Germany (1978) var første sak i EMD som omhandlet lovligheten av overvåking og lagring av data under EMK art. 8. Saksøkerne bestred ikke statens mulighet til å lovfeste overvåkingstiltak, men at lovgivningen ikke forpliktet myndigheten til å informere de berørte parter om overvåkningstiltakene i etterkant. EMD pekte på to viktige poeng. Både den teknologiske utviklingens betydning for spionasje- og overvåkingstiltak og samtidig utviklingen i trusselbildet for Europa og en økt fare for terrorisme. Retten påpekte at for at samfunnet skal kunne møte en økende fare for terrorangrep må en stat ha mulighet til å iverksette hemmelig overvåking av "uønskede elementer" i samfunnet.[168] Med dette for øye godtok retten hemmelig overvåking som et nødvendig tiltak i et demokratisk samfunn.

Klass-saken er gammel, men viser likevel avveiningen mellom retten til respekt for privatliv og fri korrespondanse på den ene siden og hensynet til bekjempelse av kriminalitet på den andre side. Da som nå var bakgrunnen for overvåkingstiltaket et (antatt) forverret trusselbilde kombinert med utviklingen innen teknologien og dens betydning for utøvelse av kriminelle handlinger.

5.2.3.2.2 Weber and Saravia v. Germany

Saken ble avgjort 29. juni 2006 og gjaldt omfanget av Federal Intelligence Service's (FIS) muligheter til å gjøre opptak av telekommunikasjon som et ledd i strategisk overvåking.

Strategisk overvåking brukes av FIS for å avdekke informasjon om telekommunikasjon som kan identifisere og avdekke alvorlige trusler mot Tyskland. Domstolen fastholder standpunktet fra liknende saker om at så lenge det finnes et lovverk som hjemler hemmelig

[168] Avsnitt 48

overvåking vil det medføre en fare for overvåking av alle som er omfattet av loven.[169] Videre at en slik fare for overvåking er å anse som et inngrep i retten til respekt for privatliv og fri kommunikasjon i EMK art. 8.

Saksøkerne mente adgangen til strategisk overvåking var blitt for stor i forhold til behovet ettersom overvåkingen ikke hadde noen geografisk begrensning og det i tillegg ville være mulig å identifisere personene samt å analysere deres bevegelser dersom de brukte mobiltelefoner.[170] De mente at den vide adgangen til strategisk overvåking ikke var nødvendig for å sikre Tyskland mot terror og internasjonalt angrep.[171] Tyske myndigheter derimot mente overvåkingen ikke kunne ses som overdreven, og at det på det gjeldende tidspunkt bare var rundt 10 % av befolkningen som anvendte mobiltelefoner og som derfor ville være i fare for overvåking. Videre fremhevet tyske myndigheter at overvåkingen i praksis var begrenset til noen få land, og at for å avdekke identiteten til sender og mottaker måtte et bestemt ord ha blitt benyttet i samtalen.[172]

EMD kom til, under henvisning til Klass and Others v. Germany (1978), at et slikt system for overvåking som det her var tale om var å anse som nødvendig i det demokratiske samfunn.

Det som gjør denne avgjørelsen anvendelig i forhold til datalagringsdirektivet er at det er tale om overvåking av mobiltelefoni uten noen geografisk begrensning og at behovet for overvåkingen ikke er direkte knyttet opp mot en spesiell trussel, men for å sikre landet mot terror og liknende angrep. Det som derimot skiller disse to tilfellene er at det i Weber og Saravia-saken kun er tale om strategisk overvåking av telekommunikasjon, mens datalagringsdirektivet også omfatter internettbruk.Videre er det i Weber og Saravia-saken kun tale om overvåking i inntil tre måneder, videre overvåking kan kun skje etter en ny

[169] Avsnitt 78

[170] Avsnitt 111

[171] Avsnitt 112

[172] Avsnitt 110

søknad.[173] Etter datalagringsdirektivet skal trafikk- og lokasjonsdata fra all elektronisk kommunikasjon lagres i minimum seks måneder og maksimum to år. I tillegg var det i Weber og Saravia-saken en filtreringsmekanisme som plukket opp bestemte ord slik at ikke all kommunikasjon ble nærmere bearbeidet.[174] Slik jeg ser det er det vesentlige forskjeller på disse to tilfellene som gjør at vurderingen av proporsjonalitetsprinsippet i forhold til datalagringsdirektivet vil bli noe annerledes. Dette synspunktet støttes også av Wessel-Aas.[175]

5.2.3.2.3 Liberty and Others v. United Kingdom

Saken gjaldt lovligheten av "Electronic Test Facility" (EFT), et system for overvåking av kommunikasjon som krysset Storbritannias grenser. Systemet ble betjent av det britiske forsvarsdepartementet på 1990-tallet. EFT var laget for å kunne oppfatte inntil 10 000 telefonsamtaler som kom fra Dublin og London og videre til kontinentet. Organisasjonene Liberty, British Irish Right Watch og Irish Council for Civil Liberties blant andre mente EFT i tiden 1990-1997 hadde snappet opp all offentlig kommunikasjon som gikk via mikrobølgefrekvenser mellom to av British Telecoms radiostasjoner. På denne frekvensen gikk det meste av Irlands telekommunikasjon og saksøkerne hadde i den angitte tidsperiode hatt regelmessig telefonisk kontakt hvor de blant annet hadde hjulpet hverandre med juridiske råd til sine klienter.[176]

For at kommunikasjonen skulle bli plukket opp av EFT ble det brukt et sorteringssystem. Det sikret at bare kommunikasjon som inneholdt visse nærmere angitte ord eller termer ville bli plukket opp av overvåkningssystemet og videre bearbeidet.[177]

---

[173] Weber and Saravia v. United Kingdom (2006) avsnitt 20

[174] Weber and Saravia v. United Kingdom (2006) avsnitt 32

[175] Wessel-Aas (2010) s. 51

[176] Avsnitt 5

[177] Avsnitt 66

Under henvisning til Weber and Saravia-saken konkluderte domstolen med at eksistensen av lovregler som tillater bruk og lagring av oppsnappet kommunikasjon utgjør et inngrep i rettighetene etter EMK art. 8 første ledd.[178]

EMD konkluderte med at den britiske lovgivningen ikke på en tilstrekkelig klar måte anga vilkårene for utøvelsen av statens skjønnsmargin ved utvelgelsen av opplysninger som skulle snappes opp. I følge domstolen var det et særlig problem at prosedyren som skulle følges ved innsamling, bearbeidelse, lagring og sletting av innsamlede opplysninger ikke var fastsatt på en slik måte at det var tilgjengelig for allmennheten. Inngrepet kunne derfor ikke sies å være i samsvar med lov og EMK art. 8 var derfor overtrådt.[179]

Som nevnt ovenfor er det også i denne saken et overvåkingssystem med en filtreringsløsning som sorterer ut hvilke kommunikasjoner som blir gjenstand for nærmere bearbeidelse. Dette skiller seg markant fra datalagringsdirektivet der all trafikk- og lokasjonsdata skal lagres, uten hensyn til kommunikasjonsformen og uten noen sorteringsmekanisme. Denne saken synes derfor heller ikke å være sammenlignbar med datalagringsdirektivet.

5.2.3.2.4 S. and Marper v. United Kingdom

I motsetning til de tre andre sakene jeg nettopp har omtalt er denne saken ikke knyttet til overvåking av kommunikasjon og lagring av denne. Dette tilfellet gjaldt lagring av fingeravtrykk og DNA-prøver fra to personer som tidligere hadde vært siktet i hver sin straffesak. Den ene (S) ble frikjent og for den andre (Marper) ble ikke siktelsen opprettholdt. Felles for disse to var at deres fingeravtrykk og DNA-prøver forble lagret mot deres vilje.

[178] Avsnitt 56

[179] Avsnitt 69

Domstolen konkluderte under henvisning til Leander v. Sweden (1987) med at lagring av data knyttet til en persons privatliv er et inngrep i rettigheten etter EMK art. 8 første ledd. Dette er uavhengig av etterfølgende bruk av de lagrede opplysningene.[180]

Motparten anførte at kravet om proporsjonalitet var klart oppfylt og baserte det på fem punkter. Fingeravtrykkene og DNA-prøvene forble lagret kun til bruk for avsløring, etterforskning og straffeforfølging i senere straffesaker, således til en begrenset bruk. Informasjonen skulle ikke benyttes uten sammenlikningsgrunnlag fra et åsted. Fingeravtrykkene skulle ikke offentliggjøres. Et utrent øye ville ikke kunne gjenkjenne en person kun med bakgrunn i det lagrede materialet og resultatet av en utvidet database ville være store fordeler for politiet i kampen mot alvorlig kriminalitet.[181]

Retten uttalte at det i dagens Europa er uomtvistet at man i kampen mot alvorlig kriminalitet og terrorisme er avhengige av vitenskapelige og tekniske nyvinninger for å kunne drive etterforskning og identifisere gjerningspersonene.[182] Imidlertid må bruken av slike etterforskningsteknikker begrenses.[183]

I S. and Marper v. United Kingdom (2008) er det ikke snakk om hvorvidt generell lagring av personopplysninger i form av fingeravtrykk og DNA-prøver er forenlig med EMK art. 8. Imidlertid er det spørsmålet om hvorvidt lagring av disse opplysningene for saksøkerenes del kan legitimeres ettersom de aldri ble straffedømt, men kun har vært mistenkt for kriminelle handlinger.

I denne saken var det ingen tidsgrense på når lagringen skulle opphøre. Opplysningene om saksøkerne kunne således risikere å bli stående til evig tid.[184] I tillegg la domstolen vekt på

[180] Avsnitt 67

[181] Avsnitt 21

[182] Avsnitt 105

[183] Avsnitt 106

[184] Avsnitt 113

at lagringen skjedde relativt vilkårlig. Forskjellene på de lagrede opplysningene (fingeravtrykk og DNA-prøver) var av mindre betydning for domstolen som vurderte dem under ett. [185]

Storbritannia hevdet på sin side at lagringen i seg selv ikke ville ha noen betydning for de registrerte så lenge den ikke medførte at de ble koblet til en straffesak i fremtiden. Dette bestred EMD som igjen slo fast at lagringen i seg selv utgjør et inngrep i retten til respekt for ens privatliv.[186]

Domstolen konkluderte med at den generelle og vilkårlige lagringen av fingeravtrykk og DNA-prøver fra personer som hadde vært mistenkt for lovbrudd, men ikke var straffedømte var i strid med EMK art. 8, og at Storbritannia med lagringen hadde overskredet statens skjønnsmargin.[187]

Det er delte meninger om hvorvidt denne avgjørelsen kan brukes i vurderingen av hvorvidt datalagringsdirektivet er i tråd med EMK art. 8 eller ikke. I nevnte sak blir det lagt stor vekt på at det britiske politiet lagret opplysninger om ikke-dømte personer på lik linje med opplysninger om straffedømte personer. Datalagringsdirektivet legger ikke opp til datalagring avhengig av en persons kriminelle rulleblad. Tvert i mot sikrer det lik lagring av opplysninger for alle impliserte. Bruce hevder at S. and Marper v. United Kingdom (2008) ikke kan tas til inntekt mot datalagringsdirektivet ettersom sistnevnte vil ramme alle personer likt og ingen grupper vil forskjellsbehandles slik som tilfellet var for S. og Marper.[188] Wessel-Aas er uenig med Bruce og mener det er flere likheter mellom lagringen som var tema i S. and Marper v. United Kingdom (2008) og datalagring slik det legges opp til i datalagringsdirektivet.[189] Av likheter peker han på at det både i nevnte dom og i

---

[185] Avsnitt 120

[186] Avsnitt 121

[187] Avsnitt 125

[188] Bruce (2010) s. 21

[189] Wessel-Aas (2010) s. 52

direktivet er tale om tvungen registrering og masselagring av personopplysninger, kun for et eventuelt fremtidig politiformål.[190] Jeg heller nok i retning av Wessel-Aas' synspunkt her.

5.2.3.3 Avgjørelsen fra den rumenske forfatningsdomstolen

Som nevnt i punkt 5.1.1 var datalagringsdirektivet oppe til behandling i den rumenske forfatningsdomstolen i 2009. I den rumenske implementeringen av direktivet er det fastsatt en lagringstid på seks måneder. I den rumenske loven som er ment å gjennomføre direktivet inkluderes trafikk- og lokasjonsdata fra fysiske og juridiske personer: *"the related data necessary for the identification of the subscriber or registered user"*[191] uten at *"related data"* er konkretisert nærmere. Dette er identisk med ordlyden i datalagringsdirektivet art. 1 annet ledd, men ble likevel kritisert av forfatningsdomstolen i Romania. Domstolen mente at mangelen på en presis formulering åpner for misbruk ved lagring og behandling av opplysninger lagret av tilbydere av elektronisk kommunikasjon. En vagt formulert lovtekst vanskeliggjør borgernes forutsigbarhet med tanke på et eventuelt overtramp av regelen. Et annet aspekt ved implementeringen som ble tillagt vekt av domstolen var konseptet med uavbrutt lagring. Fra kommunikasjonen skjer er tilbyderne forpliktet til å lagre trafikk- og lokasjonsdata i seks måneder uten mulighet til å avslutte lagringen, noe domstolen mener er en fortsatt begrensning av en persons privatliv og frie kommunikasjon. Eneste mulighet for fri og usensurert kommunikasjon vil således være direkte kommunikasjon, noe som må anses upraktisk i dagens teknologiske samfunn. Domstolen ser hensynet bak loven, og forstår at det er behov for å sikre tilstrekkelige verktøy for å oppklare alvorlig kriminalitet i lys av den teknologiske utviklingen. Likevel mener domstolen etter en helhetsvurdering at implementeringen av datalagringsdirektivet ikke kan forsvarers ut fra proporsjonalitetsprinsippet.[192]

---

[190] Wessel-Aas (2010) s. 159

[191] Romania Constitutional Court, Decision no. 1258, 08.10.2009, avsnitt 1

[192] Romania Constitutional Court, Decision no. 1258, 08.10.2009

5.2.3.4 Avgjørelsen fra den tyske forfatningsdomstolen

Datalagringsdirektivet har også vært oppe til behandling i den tyske forfatningsdomstolen. Her var det imidlertid måten direktivet var implementert på som voldte problemer, ikke datalagring i seg selv.

Slik datalagringsdirektivet er implementert i Tyskland gjennom den tyske straffeprosessloven og den tyske telekommunikasjonsloven kom retten til at prinsippet om forholdsmessighet ikke er tilstrekkelig ivaretatt. Videre uttaler domstolen at implementeringen heller ikke oppfyller kravene til datasikkerhet eller sikrer en begrensning i bruken av de lagrede dataene, og at implementeringen totalt sett derfor strider mot den tyske grunnloven.[193] Det ble lagt vekt på at ved en slik omfattende lagring av data måtte lovgivningen sørge for tilstrekkelig datasikkerhet for å kunne oppfylle vilkåret om forholdsmessighet. Slik direktivet er implementert i Tyskland hjemler den tyske straffeprosessloven innhenting av data ved enhver forbrytelse begått ved hjelp av telekommunikasjon, uavhengig av alvorlighetsgraden.[194] Ved en så generell bestemmelse vil lagrede data kunne benyttes ved etterforskning av omtrent alle forbrytelser, og den tyske telekommunikasjonsloven går dermed betraktelig lengre enn datalagringsdirektivet som er begrenset til etterforsking, oppklaring og straffeforfølging av alvorlig kriminalitet, jfr. direktivets art. 3. Resultatet i Tyskland ble på bakgrunn av de ovenfor nevnte momenter at lovbestemmelsene som er ment å implementere datalagringsdirektivet er ugyldige, og følgelig at opplysninger lagret i medhold av disse bestemmelsene måtte slettes.[195]

5.2.3.5 Finnes det andre alternativer?

Art. 29 WP har påpekt at det finnes andre løsninger som er ansett å være mindre inngripende enn datalagringsdirektivet, som for eksempel den såkalte ”quick freeze procedure”. Den løsningen går ut på at når politiet har en mistenkt, men fortsatt mangler

[193] Press release, Federal Constitutional Court of Germany, s. 3

[194] Press release, Federal Constitutional Court of Germany, s. 9

[195] Press release, Federal Constitutional Court of Germany, s. 12

bevis kan de pålegge tilbyder av elektronisk kommunikasjon å lagre kommunikasjonsdata om den mistenkte. Da har politiet mulighet til på et senere tidspunkt få en rettslig kjennelse på utlevering av de lagrede dataene.[196] Hvorvidt dette kan være en bedre måte å sikre bevis på for politiet har jeg ikke grunnlag for å vurdere. Derimot viser praksis fra EMD at såkalt strategisk overvåking kan være forenlig med EMK art. 8.[197] I disse tilfellene er det overvåkingssystemer med filtreringsmekanismer som effektivt siler ut de deler av informasjonen som fanges opp som ikke skal være gjenstand for videre behandling. Sorteringsmekanismen kan for eksempel være slik at informasjonen må inneholde visse ord for å bli fanget opp. FRA-loven[198] som er innført i Sverige er et eksempel på en slik løsning.

5.2.3.6 Forholdet til den svenske FRA-loven

FRA-loven åpner for at svenske myndigheter har anledning til å drive signalspaning på all elektronisk kommunikasjon, både trådløs og trådbunden, som krysser Sveriges grenser.[199] FRA-loven kom som følge av etteretningsmessige hensyn i forhold til terrorisme og internasjonal kriminalitet. FRA-loven kan minne om datalagringsdirektivet. Etter FRA-loven er det også kun trafikkdata som kan lagres i stor utstrekning, den hjemler ikke lagring av innholdsdata. All informasjon som passerer de svenske riksgrensene vil rutes/lagres og FRA[200] -systemet får tilgang til informasjonen. Noe av denne informasjonen kan etter en grov- og finsortering avlyttes og bearbeides nærmere.[201] FRA-loven har så langt ikke vært til vurdering i EMD. Lund mener at den svenske loven skiller seg fra datalagringsdirektivet ved at det etter FRA-loven er utskillingsmekanismer som kan skille ut relevant informasjon, og ikke en udiskriminert lagring av all trafikkdata.[202]

---

[196] Bignami (2007) s. 249

[197] Weber and Saravia v. Germany (2006)

[198] Lov om signalspaning i forsvarsetteretningsvirksomhet, vedtatt av den svenske Riksdagen 18. juni 2008

[199] Lund (2010)

[200] Forsvarets Radioanstalt, svensk etteretning

[201] Lund (2010)

[202] Lund (2010)

5.3 Implementering av datalagringsdirektivet i andre land

Ettersom fristen for implementering av datalagringsdirektivet har gått ut har de fleste EU-land implementert direktivet. De land som enda ikke har implementert direktivet er Sverige, Irland, Hellas og Østerrike.[203]

Danmark implementerte direktivet med *bekendtgørelse nr. 988 af 28/09/2006* og det trådte i kraft 15. september 2007. I Danmark har man valgt en lagringstid for teletrafikk på ett år. Utlevering til politiet kan skje i henhold til den danske retsplejeloven og kun når visse vilkår er oppfylt. Det må for det første være bestemte grunner til å tro at den mistenkte benytter de kommunikasjonsmidler utleveringen gjelder og en utlevering må være av avgjørende betydning for sakens oppklaring. Videre kan utlevering kun skje ved etterforskning av en handling som har minst seks års strafferamme eller den rammes av visse opplistede lovregler, som blant annet terrorisme og barnepornografi. Data knyttet til et konkret geografisk område kan imidlertid kun utleveres dersom det er fare for liv og helse. Endelig kan utlevering kun skje når det er et forholdsmessig tiltak i forhold til formålet, sakens betydning og ulempene for de impliserte. Normalt kan opplysningene ikke benyttes som bevis i en annen sak enn de opprinnelig ble utlevert for. I Danmark er det også nedsatt en arbeidsgruppe som skal se på utfordringen ved uregistrerte brukere ved internettkafeer, biblioteker og gratis trådløse soner.[204]

I Finland ble datalagringsdirektivet implementert ved en endring i *lag om dataskydd vid elektronisk kommunikation* med ikrafttredelse 1. juni 2008. Også i Finland er det valgt en lagringstid på ett år. Tidligere var finske tilbydere bare pålagt å lagre data for forretningsmessige formål. Utlevering av de lagrede data kan kun skje i forbindelse med etterforskning og det må være en skjellig grunn til mistanke om lovbrudd som har minst

[203] Samferdselsdepartementets høringsnotat s. 22

[204] Samferdselsdepartementets høringsnotat s. 20-21

fire års strafferamme, med mindre det gjelder mistanke om datakriminalitet, hallikvirksomhet, trusler, narkotikaforbrytelser eller terrorisme.[205]

I Sverige er datalagringsdirektivet enda ikke innført, men det har vært gjennomført en utredningsprosess der det har blitt undersøkt hvordan implementeringen av direktivet kan skje. Det er i utredningen foreslått en lagringstid på ett år. I dag er det likevel mulig for svensk politi å få utlevert data så lenge det skjer etter beslutning fra retten og det foreligger mistanke om datakriminalitet, narkotikaforbrytelser, grove tilfeller av barnepornografi eller annen straffbar handling med minst seks måneders strafferamme. I medhold av den svenske ekomloven kan påtalemyndigheten også få utlevert data, men kun når det er tale om lovbrudd med minst to års strafferamme.[206] I tillegg eksisterer det allerede en form for datalagring i Sverige som følge av FRA-loven.[207]

Av landene som har implementert direktivet har den største gruppen valgt ett års lagringstid. I Tyskland og Romania har man valgt seks måneders lagringstid, og i begge disse landene har direktivet vært omdiskutert og gjenstand for rettslig behandling.[208] I begge land kom de respektive forfatningsdomstoler til at implementeringen var uforenlig med intern rett.[209] Irland anla sak for EU-domstolen med påstand om at direktivet var vedtatt med feil hjemmel, men tapte saken og har siden implementert direktivet.[210]

---

[205] Samferdselsdepartementets høringsnotat s. 21

[206] Samferdselsdepartementets høringsnotat s. 22

[207] Se punkt 5.2.3.6

[208] Romania Constitutional Court, decision no.1258 og press release, Federal Constitutional Court of Germany

[209] Se punkt 5.1.1, 5.2.3.3 og 5.2.3.4

[210] Sak C-301/06 Irland mot Europa-parlamentet og Rådet for Den Europeiske Union

5.4 Rettspolitiske betraktninger

5.4.1 Fare for misbruk

Ved lagring av opplysninger vil det alltid være en fare for misbruk. Lagring av trafikk- og lokasjonsdata er intet unntak. Det vil ikke være mulig å garantere at ingen kommer til å misbruke opplysningene som lagres i medhold av datalagringsdirektivet. Opplysninger som lagres elektronisk vil kunne bli avslørt av personer som bryter seg inn i systemet. Etter datalagringsdirektivet art. 1 skal tilbydere av offentlig kommunikasjonsnett eller -tjeneste lagre dataene. Hvorvidt dataene skal lagres hos tilbyder eller i en sentral database ved en implementering av direktivet i Norge er ikke avklart. Foreløpig har Samferdselsdepartementet åpnet for at tilbyderne selv skal kunne velge det mest hensiktsmessige lagringsstedet.[211] Etter mitt syn vil faren for misbruk eksistere uavhengig av hvor opplysningene lagres rent fysisk.

Det finnes allerede eksempler på at informasjon lagret hos teletilbydere er blitt gjenstand for misbruk.[212] I Hellas fikk en person tak i informasjon om flere hundre personer etter å ha tatt seg inn hos teleselskapet Vodafone, samme år skjedde en liknende lekkasje fra det italienske teleselskapet Telecom. I 2005 ble fem personer som var ansatt i teleselskapet Sonera i Finland dømt for å ha tatt ut opplysninger lagret hos selskapet. I 2008 valgte det tyske teleselskapet Telekom å overvåke styremedlemmer og journalister for å avsløre hvem som ga opplysninger videre til journalistene.[213] I 2007 var det datainnbrudd hos teleselskapet Tele2, og en rekke personopplysninger ble i løpet av en tre dagers periode "høstet inn" av uvedkommende.[214] Eksemplene viser at faren for misbruk ved lagring av personopplysninger absolutt er tilstede.

---

[211] Samferdsels departementets høringsnotat s. 38

[212] Flyghed (2009)

[213] Flyghed (2009)

[214] TAHER-2009-118388 (Lovdata)

En annen type ”misbruk” som kan tenkes i kjølvannet av en eventuell implementering av datalagringsdirektivet er muligheten for å ”plante bevis”. At en person X heller benytter seg av telefonen til Y eller bruk av andres datamaskin ved oppkobling mot Internett kan etter mitt syn ikke ses som utenkelig. Dette er en bekymring som ICJ Norge (Den internasjonale juristkommisjon, norsk avdeling) deler.[215]

5.4.2 Overskuddinformasjon

Hvor mye av den lagrede informasjonen som faktisk vil bli brukt av politiet for å etterforske og oppklare alvorlig kriminalitet er ikke nøyaktig tallfestet. Ved en slik masselagring som datalagringsdirektivet legger opp til vil nødvendigvis en stor andel av de lagrede opplysningene bli å regne som overskuddsinformasjon. At det skal lagres en stor mengde overskuddsinformasjon i minst seks måneder og kanskje opp mot to år er etter min mening uheldig.

[215] Brev: ICJ-Norges syn og anbefalinger rundt datalagringsdirektivet

6 Konklusjon

I denne delen vil jeg forsøke å komme med en oppsummering og konklusjon på problemstillingen, om hvorvidt lagringsplikten etter datalagringsdirektivet, herunder lagringstid og hva som skal lagres er i strid med retten til respekt for privatliv og korrespondanse i EMK art 8.

Som redegjort for i punkt 5.2.3.1 er det et visst behov for lagring av trafikkdata. Det må antas at dette behovet vil bli økende i fremtiden, dersom det blir slutt på fakturering av teletjenester basert på forbruk. Terroranslag som bombene i Madrid i 2004 og i London i 2005 har vist et økt trusselbilde for Europa og er bakgrunnen for tilblivelsen av datalagringsdirektivet. Tilgang på historiske trafikkdata kan i en del slike tilfeller være eneste mulighet til å avsløre kriminelle nettverk.[216]

Selv om et formål i seg selv er saklig er det ikke automatisk proporsjonalitet mellom formålet og den konkrete behandling av personopplysninger.[217] I medhold av datalagringsdirektivet vil det lagres mye informasjon om mennesker som på ingen måte utgjør noen trussel for samfunnet. Disse personene vil da få innskrenket sine rettigheter etter EMK art. 8 uten at det er nødvendig. I doktoravhandlingen til Bagger Tranberg brukes et liknende eksempel: ”*Dette vil være tilfældet, hvis der innsamles og opbevares oplysninger om en stor del af den danske befolkning med det formål at lette eksempelvis en tilmeldingssituation for en mindre del af befolkningen.”*[218]

[216] Blume (2002) s. 87

[217] Bagger Tranberg (2007) s. 545

[218] Bagger Tranberg (2007) s. 545

Omfattende datalagring reiser spørsmål rundt den enkeltes rettigheter etter EMK art. 8. Som redegjort for i oppgavens kapittel 5 vil lagring i seg selv utgjøre et inngrep i retten til respekt for privatliv og korrespondanse. Masselagring av opplysninger vil dessuten alltid være forbundet med en fare for misbruk. [219]

Det har ikke vært mulig å finne noen statistikk for at økt lagring av opplysninger som foreskrevet i datalagringsdirektivet vil medføre noen økt oppklaringsgrad for alvorlig kriminalitet i Norge.[220] Uten noen konkrete holdepunkter for at datalagringsdirektivet vil øke oppklaringsgraden av alvorlig kriminalitet kan direktivet i mine øyne vanskelig oppfylle kravet om forholdsmessighet i EMK art. 8 annet ledd.

Avgjørelser fra EMD, som er redegjort for under punkt 5.2.3.2, viser også at lagring av personopplysninger kan være problematisk. S. and Marper v. United Kingdom (2008) viser at hvorvidt opplysningene som lagres vil bli brukt i fremtiden eller ikke, er av mindre betydning ved vurdering av forholdsmessigheten ved tiltaket.

Den rumenske forfatningsdomstolen la i sin vurdering av datalagringsdirektivet vekt på at direktivet la opp til en fortsatt lagring og at trafikk- og lokasjonsdata om all kommunikasjon skulle lagres i seks måneder.[221] Datalagringsdirektivet var til behandling hos den tyske forfatningsdomstolen, som konkluderte med at den tyske implementeringen var i strid med den tyske grunnloven på grunn av manglende forholdsmessighet. Det ble blant annet lagt vekt på at lovgiver ikke hadde sørget for tilstrekkelige datasikkerhetstiltak i forhold til den mengden datalagring implementeringen la opp til.[222]

---

[219] Willassen (2010) s. 8 og punkt 5.4.1

[220] Se punkt 5.2.3.1

[221] Se punkt 5.2.3.3

[222] Se punkt 5.2.3.4

Datalagringsdirektivet har i motsetning til den svenske FRA-loven ingen filtreringsmekanisme som kan plukke opp relevante opplysninger, men legger i stedet opp til en ukritisk masselagring som går ut over rettighetene til en hel befolkning.

På bakgrunn av tidligere EMD-praksis kan det utledes at lagring av trafikkdata passerer kravet om forholdsmessighet i EMK art 8 annet ledd dersom det eksisterer en sorteringsmekanisme som plukker ut hvilke opplysninger som skal bearbeides. På den annen side er en generell masselagring av personopplysninger ikke i tråd med forholdsmessighetskravet, jfr. S. and Marper v. United Kingdom (2008). Etter min mening vil også lagringstiden by på problemer i forhold til forholdsmessighetskravet. Dette kan illustreres ved avgjørelsen i den rumenske forfatningsdomstolen. Bestemmelsene i datalagringsdirektivet legger opp til en omfattende lagring av trafikk- og lokasjonsdata uten noen form for en sorteringsmekanisme. Som tidligere nevnt er det ikke konkrete holdepunkter for at bestemmelsene i datalagringsdirektivet vil medføre økt oppklaring av alvorlig kriminalitet. På bakgrunn av disse betraktningene kan det etter mitt syn utledes at bestemmelsene i datalagringsdirektivet ikke oppfyller kravet om forholdsmessighet i EMK art. 8 annet ledd.

7 Litteraturliste

7.1 Lovgivning

7.1.1 Norske lover og forskrifter

1899 Lov om Eneret for Staten til Befordring af Meddelelse ved Hjælp af Telegraflinjer og lignende Anlæg (telegrafloven) av 29. april 1899 (opphevet)

1902 Alminnelig borgerlig Straffelov (straffeloven) av 22. mai 1902 nr. 10

1978 Lov om personregistre m.m. (personregisterloven) av 9. juni 1978 nr. 48 (opphevet)

1981 Lov om rettergangsmåten i straffesaker (straffeprosessloven) av 22. mai 1981 nr. 25

1992 Avtale om Det europeiske økonomiske samarbeidsområde (EØS-avtalen) av 27. november 1992 nr. 109

1995 Lov om telekommunikasjon (teleloven) av 23. juni 1995 nr. 39 (opphevet)

1999 Lov om styrking av menneskerettighetenes stilling i norsk rett (menneskerettsloven) av 21. mai 1999 nr. 30

2000 Lov om behandling av personopplysninger (personopplysningsloven) av 14. april 2000 nr. 31

2003 Lov om elektronisk kommunikasjon (ekomloven) av 4 juli 2003 nr. 83

2005 Lov om endringer i straffeloven og straffeprosessloven og om samtykke til ratifikasjon av Europarådets konvensjon 8. november 2001 om bekjempelse av kriminalitet som knytter seg til informasjons- og kommunikasjonsteknologi (lovtiltak mot datakriminalitet) av 8. april 2005 nr. 16

2000 Forskrift om behandling av personopplysninger (personopplysningsforskriften) av 15. desember 2000 nr. 1265

2004 Forskrift om elektronisk kommunikasjonsnett og elektronisk kommunikasjonstjeneste (ekomforskriften) av 16. februar 2004 nr. 401

7.1.2 Traktater og konvensjoner

EMK Den europeiske menneskerettskonvensjonen, Roma 1950

SP Den internasjonale konvensjonen om sivile og politiske rettigheter

TEUF Traktaten om den europeiske unions funksjonsområde

Lisboa-traktaten Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, Lisboa 2007

7.1.3 EU direktiver

EP/Rdir 1995/46/EF Europaparlaments- og rådsdirektiv 95/46/EF av 24. oktober 1995 om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger (personverndirektivet)

EP/Rdir 2002/58/EF Europaparlaments- og rådsdirektiv av 12. juli 2002 om behandling av personopplysninger og personvern i sektoren for elektronisk kommunikasjon (direktivet om personvern og elektronisk kommunikasjon)

EP/Rdir 2006/24/EF Europaparlamentets- og rådsdirektiv af 15. mart.s 2006 om lagring af data genereret eller behandlet i forbindelse med tilvejebringelse af offentlig tilgængelige elektroniske kommunikasjonsnet og om ændring af direktiv 2002/58/EF

Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws

7.1.4 Utenlandske lover

Constitution of Romania, funnet her:
http://www.cdep.ro/pls/dic/site.page?den=act2_2&par1=2#t2c2s0a28 [29. Mars 2010]

FRA-loven, Lov om signalspaning i forsvarsetteretningsvirksomhet, vedtatt av den svenske Riksdagen 18. juni 2008

7.2 Forarbeider

Ot.prp.nr. 92 (1998-1999) Om lov om behandling av personopplysninger (personopplysingsloven)

Ot.prp.nr. 58 (2002-2003) Om lov om elektronisk kommunikasjon (ekomloven)

7.2.1 Offentlige utredninger

NOU 1997:19 Et bedre personvern

NOU 2009:1 Individ og integritet

7.3 Rettsavgjørelser

7.3.1 Norske avgjørelser

Rt. 1896 s. 530 (Aarsdommen)

Rt. 1952 s. 1217 (Personverndommen)

Rt. 1964 s. 609 (Hunton Bruk)

Rt. 1982 s. 588 (Kjevikdommen)

Rt. 1991s. 616

Rt. 1998 s. 1638

Rt. 1999 s. 1944

Rt. 1999 s. 2063

Rt. 2006 s. 486 (Gardermoen)

LB-2008-61703

TAHER-2009-118388

PVN-2004-1 (Lovdata)

PVN-2005-6 (Lovdata)

PVN-2007-7 (Lovdata)

7.3.2 Internasjonale avgjørelser

Handyside v. United Kingdom, The European Court of Human Rights, Strasbourg, 7. desember 1976

Klass and Others v. Germany, The European Court of Human rights, Strasbourg, 6. september 1978

Sunday Times v. United Kingdom, The European Court of Human Rights, Strasbourg 26. april 1979

Silver and Others v. United Kingdom, The European Court of Human Rights, Strasbourg, 25. mars 1983 og Report of the Commission, 11. oktober 1980

Malone v. United Kingdom, The European Court of Human Rights, Strasbourg, 2. august 1984

Leander v. Sweden, The European Court of Human Rights, Strasbourg, 26. mars 1987

Olsson v. Sweden, The European court of Human Rights, Strasbourg, 24. mars 1988

Niemietz v. Germany, The European Court of Human Rights, Strasbourg, 16. desember 1992

Halford v. United Kingdom, The European Court of Human Rights, Strasbourg 25. juni 1997

P.G. and J.H. v. United Kingdom, The European Court of Human Rights, Strasbourg 25. september 2001

Peck v. United Kingdom, The European Court of Human Rights, Strasbourg, 28. januar 2003

Von Hannover v. Germany, The European Court of Human Rights, Strasbourg, 24. juni 2004

Weber and Saravia v. Germany, The European Court of Human Rights, Strasbourg, 29. juni 2006

Giacomelli v. Italy, The European Court of Human Rights, Strasbourg 2. november 2006

Copland v. United Kingdom, The European Court of Human Rights, Strasbourg 3. april 2007

Liberty and Others v. United Kingdom, The European Court of Human Rights, Strasbourg, 1. juli 2008

K.U. v. Finland, The European Court of Human Rights, Strasbourg 2. desember 2008

S. and Marper v. United Kingdom, The European Court of Human Rights, Strasbourg 4. desember 2008

7.3.3 EF/EØS-dommer

Sak C-101/01 Lindqvist (Lovdata)

Sak C-301/06 Irland mot Europa-parlamentet og Rådet for Den Europeiske Union (Lovdata)

7.3.4 Utenlandske dommer

Romania Constitutional Court, Decision no. 1258 from 8 October 2009 (uoffisiell oversettelse, hentet fra http://www.legi-internet.ro/english/jurisprudenta-it-romania/decizii-it/romanian-constitutional-court-decision-regarding-data-retention.html) [sitert 25. mars 2010]

7.4 Bøker

7.4.1 Nasjonale bøker

Bing, Jon. *Det ulovfestede personvern relatert til en kommunikasjonsmodell.* I: Rettsteori og rettsliv, Festskrift til Carsten Smith til 70-årsdagen 13. juli 2002, Oslo (Universitetsforlaget) s. 97-111.

Høstmælingen, Njål. *Internasjonale menneskerettigheter.* Oslo, 2003.

Ruud, Morten og Geir Ulfstein. *Innføring i folkerett.* 2. utg. Oslo, 2002.

Schartum, Dag Wiese og Lee A. Bygrave. *Personvern i informasjonssamfunnet.* 1. utg. Oslo, 2004.

Teknologirådet. *Sikkerhet og personvern. Oversikt over sikkerhetsteknologier.* Oslo, 2007. (Rapport 2 2007)

Tokvam, Ole. *Personvern og straffeansvar – straffelovens § 390.* Oslo, 1995

7.4.2 Internasjonale bøker

Bagger Tranberg, Charlotte. *Nødvendig behandling av personopplysninger.* 1. utg. København, 2007.

Blume, Peter. *Anonymitet - overvågning - tillid.* Stockholm, 2003.

Harris, David, Michael O'Boyle og Colin Warbrick. *Law of the European Convention on Human Rights. Second Edition.* 2. utg. Oxford, 2009.

Janis, Mark W, Richard S. Kay og Anthony W. Bradley. *European Human Rights Law.* 3. utg. Oxford, 2008.

Ruiz, Blanca R. *Privacy in telecommunication. A European and an American approach.* 1. utg. Dordrecht, Nederland, 1997.

Walden, Ian. *Telecommunications Law and Regulation.* 3. utg. Oxford, 2009.

Yourow, Howard Charles. *The Margin of Appreciation Doctrine in the Dynamics of European Human Rights Jurisprudence.* Dordrecht, Nederland, 1996

7.5 Artikler

7.5.1 Nasjonale tidsskriftsartikler

Bing, Jon. *Personvern, ytringsfrihet og IP-adresser.* I: Lov&Data, nr. 98, juni 2009

Bruce, Ingvild. *Datalagringsdirektivet – en menneskerettskrenkelse eller -forpliktelse?* I: Lov og Rett, Årg. 49 (2010), s. 6-26

Flyghed, Janne. *Vågar du lyfta luren nu?* I: Lov&Data, nr. 98, juni 2009

Wessel-Aas, Jon. *EUs datalagringsdirektiv – et angrep på den liberale rettstaten etter et nødvendig tiltak i moderne kriminalitetsbekjempelse.* I: Pacta, Årg.4 (2010), s. 47-53

Wessel-Aas, Jon. *Datalagringsdirektivet og EMK – kommentarer til Ingvild Bruce.* I: Lov og rett, Årg. 49 (2010), s. 154-164

7.5.2 Internasjonale tidsskriftsartikler

Bignami, Fransesca. *Privacy and Law Enforcement in the European Union: The Data Retention Directive.* I: Chicago Journal of International Law, Vol. 8, No. 1. 2007, s. 233-255

Breyer, Patrick. *Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR.* I: European Law Journal, Vol. 11, No. 3. 2005, s. 365-375

Bygrave, Lee A. *Data Protection Pursuant to the Right to Privacy in Human Rights Treaties.* I: International Journal of Law and Information Technology, Vol 6 No 3. 1998, s. 247-284

7.6 Nettdokument

Datatilsynet. *Konsesjon teletjenester med merknader.* http://www.datatilsynet.no/upload/Dokumenter/konsesjoner/konsesjon_tele_m_merkn.pdf [sitert 23. februar 2010].

Datatilsynet. *Forfatningsstridig datalagring i Tyskland.* http://www.datatilsynet.no/templates/Page____3356.aspx [sitert 29. mars 2010]

Datatilsynet. *Høringsuttalelse – implementering av datalagringsdirektivet (2006/24/EC).* http://datatilsynet.no/upload/hoering/2010/hoering_datalagring.pdf [lastet ned 23. mars 2010]

Datatilsynet. *Internasjonalt arbeid.* http://datatilsynet.no/templates/Page____399.aspx [sitert 10. april 2010]

Datatilsynet. *Lagring av IP-adresse og abonnement – informasjon (brev til IKT Norge 13. mai 2009)* http://www.datatilsynet.no/upload/tilsynsrapporter/2008/Microsoft%20Word%20-%2009-00699-1%20Lagring%20av%20IP-adresse%20og%20abonnement.pdf [lastet ned 23. april 2010]

Datatilsynet. *Om datatilsynet.* http://www.datatilsynet.no/templates/AboutPage____220.aspx [sitert 9. april 2010]

Den internasjonale juristkommisjon, norsk avdeling - ICJ-Norge. *Datalagringsdirektivet – ICJ-Norges syn og anbefalinger.* http://www.datatilsynet.no/upload/Dokumenter/saker/2009/Document.pdf [lastet ned 25. mars 2010]

Fornyings-, administrasjons- og kirkedepartementet. *Pressemelding 25.05.2007.* http://www.regjeringen.no/nb/dep/fad/pressesenter/pressemeldinger/2007/lunde-leder-av-personvernkommisjonen.html?id=468399 [sitert 9. april 2010]

Samferdselsdepartementet. *Høringsnotat datalagring.* http://www.regjeringen.no/pages/2281081/hnotat_datalagring.pdf [lastet ned 5. mars 2010]

Svein Willassen AS. *Datalagringsdirektivet – verdi i etterforskning og risikofaktorer for personvern.* Rapport utarbeidet på oppdrag fra Datatilsynet. http://datatilsynet.no/upload/Dokumenter/publikasjoner/rapporter/utredning-datatilsynet.pdf [lastet ned 11. april 2010]

Article 29 Working Party. *Udtalelse 4/2005 om forslag til Europa-Parlamentets direktiv om lagring af data behandlet i forbindelse med tilvejebringelse av offentlige elektroniske kommunikationstjenester og om ændring af direktiv 2002/58/EF.* http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp113_da.pdf [sitert 18. mars 2010]

Article 29 Working Party. *Udtalelse 3/2006 om Europa-Parlamentets og Rådets direktiv 2006/24/EF om lagring af data genereret eller ehandlet i forbindelse med tilvejebringelse af offentligt tilgjængelige elektroniske kommunikationstjenester eller elektroniske kommunikationsnet og om ændring af direktiv 2002/58/EF.*

http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp119_da.pdf [sitert 24. mars 2010]

Press release, Federal Constitutional Court, No. 11/2010 of 2 March 2010. http://www.datatilsynet.no/upload/Dokumenter/dommer/pressrelease_dataretention_bundesverfassungsgericht.pdf [sitert 29. mars 2010]

Arnesen, Finn og Fredrik Sejersted. *Om datalagringsdirektivets EØS-rettslige relevans.* Oslo 2009. http://www.regjeringen.no/pages/2281081/Betenkning_datalagring_Arnesen_og_Sejersted_2009-januar.pdf [sitert 11. mars 2010]

Haugland, Geir Sunde. *Kommentar til straffeprosessloven.* I: Norsk Lovkommentar nettversjon. [sitert 2. mars 2010]

Nordeide, Ragnar. *Kommentar til EMK.* I: Norsk Lovkommentar nettversjon. [sitert 19. januar 2010].

Rønnevig, Leif-Henrik. *Kommentar til ekomloven.* I: Norsk Lovkommentar nettversjon. [sitert 5. februar 2010]

Schartum, Dag Wiese. *Kommentar til personopplysningsloven.* I: Norsk Lovkommentar nettversjon. [sitert 28. januar 2010]

Skaflem, Ingolf. *Kommentar til straffeprosessloven.* I: Norsk Lovkommentar nettversjon. [sitert 1. mars 2010]

7.7 Personlige meddelelser

Apenes, Georg. Foredrag på seminar om datalagringsdirektivet i regi av Norsk forening for jus og edb. 2. mars 2010.

Lund, Ketil. Foredrag på seminar om datalagringsdirektivet i regi av Norsk forening for jus og edb 2. mars 2010.